

S. HRG. 113-326

OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED THIRTEENTH CONGRESS SECOND SESSION

WEDNESDAY, JUNE 19, 2013

Serial No. J-113-18

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE
88-484 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California	CHUCK GRASSLEY, Iowa, <i>Ranking Member</i>
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	JEFF FLAKE, Arizona
MAZIE HIRONO, Hawaii	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE CHAIR

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	42
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa	3

WITNESSES

Witness List	41
Mueller, Hon. Robert S. III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC	6
prepared statement	44

QUESTIONS

Questions submitted by Senator Sheldon Whitehouse for Hon. Robert S. Mueller III	58
Questions submitted by Senator Charles Grassley for Hon. Robert S. Mueller III	59
Questions submitted by Senator Orrin Hatch for Hon. Robert S. Mueller III	71

ANSWERS

Responses of Hon. Robert S. Mueller III to questions submitted by Senators Whitehouse, Grassley, and Hatch	72
---	----

**OVERSIGHT OF THE FEDERAL BUREAU OF
INVESTIGATION**
WEDNESDAY, JUNE 19, 2013

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in Room SD-226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feinstein, Durbin, Whitehouse, Klobuchar, Franken, Hirono, Grassley, Hatch, Sessions, Lee, Cruz, and Flake.

**OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S.
SENATOR FROM THE STATE OF VERMONT**

Chairman LEAHY. Good morning. Today the Judiciary Committee welcomes Robert Mueller for what is likely to be his final appearance before this panel as Director of the Federal Bureau of Investigation.

As we know, Director Mueller began as head of the FBI just days before the terrorist attacks of September 11, 2001.

And, Director, I remember being down in your Intelligence Center at the FBI building right after that and going over, still sifting, what we knew and actually what we did not know about that attack.

For nearly 12 years, he has led the Bureau as it has shifted its primary focus to national security and counterterrorism efforts while still carrying on the historic mission of fighting crime. And that transition, while important for our national security, of course, has had, as expected, some problems. From National Security Letters to the latest revelations about the use of the PATRIOT Act, I remain concerned that as a country we have yet to strike the right balance between the intelligence-gathering needs of the FBI and the civil liberties and privacy rights of Americans. I also want to make sure that the shift, while necessary, in the FBI's focus does not unduly hamper the Bureau's ability to investigate cases involving fraud and violent crime that significantly affect the everyday lives of Americans.

These are concerns I express, but I think one thing that the Director knows and the public knows, I have never questioned the integrity, the dedication, and the consummate professionalism of Director Mueller as he has led the Bureau through very difficult times. He has been a steady and determined leader of the FBI. He has spoken forcefully about the need to protect Americans' civil liberties, and I remember sitting there at the 100th anniversary of the Bureau and the Director's very strong statement about the civil

liberties of all Americans. And it was no surprise that a committed public servant like Bob Mueller would agree to put his long-awaited vacation and travel plans on hold when the President asked him to stay on board for another two years. He has devoted his entire life to public service. We were just talking about how Senator Feinstein knew him during a very terrible time, at the time when she became mayor of San Francisco with the tragedies that led up to that. And we are grateful to him and his family for their continued sacrifice.

I might mention in this regard, Director Mueller, your wife, Ann, she is—I know what she has put up with, with the absences and all. You have a wonderful family. I have had the privilege of meeting them. But I hope you will tell Ann also how much I and the others appreciate what she has done, too, to make it possible for you to be Director. You are going to leave enormous shoes to fill.

As the FBI now prepares for its first change in leadership since the 9/11 attacks, we have to review closely the broad intelligence-gathering powers that Congress granted the FBI. They face daunting national security challenges, but we also have to ensure—and this is the responsibility of not only the FBI but the oversight—that they do not violate the privacy rights and civil liberties of law-abiding Americans. I have long said that protecting national security and protecting Americans' fundamental rights are not mutually exclusive. We can and we must do both.

The recent public revelations about two classified data collection programs illustrate the need for close scrutiny by Congress of the government's surveillance activities. I have been troubled for years by the expansive nature of the *USA PATRIOT Act*. These powerful law enforcement tools, including Section 215 orders, require careful monitoring. That is why I authored legislation in 2009 that would have improved and reformed the *PATRIOT Act* while also increasing its transparency. My bill was reported by this Committee on a bipartisan basis in 2009 and 2011. I intend to reintroduce—just so everybody will know, I am going to reintroduce that bill tomorrow and hope that Senators from both parties will join me in this effort to improve the *PATRIOT Act*.

The American people deserve to know how broad investigative laws like the *PATRIOT Act* are being interpreted and used to conduct electronic surveillance. Americans also deserve to know whether these programs have proven sufficiently effective to justify their breadth. Right now, I have to state I remain skeptical.

I also firmly believe that we need to maintain close oversight over the broad surveillance authorities contained in the *FISA Amendments Act*. I have had concerns about the scope of Section 702, even though its statutory focus is on foreigners overseas. That is why I pushed for a shorter sunset, greater transparency, and better oversight last year when Congress considered reauthorizing these provisions. I regret that the Senate rejected my efforts. I think now there is a possibility they may in further legislation accept these commonsense improvements.

We have to have an open debate about the efficacy of these tools, particularly in light of the Boston Marathon bombing in April, not only how we collect it but what we do with it once it is collected, whether intelligence obtained by the FBI had been properly relayed

through the Joint Terrorism Task Force to the Boston Police Department. There have been questions raised that it was not. And I know the Inspector General for the intelligence community is conducting an independent assessment.

Finally, the FBI's increased focus on counterterrorism cannot come at the expense of the regular law enforcement efforts. Preliminary data released earlier this month show that in 2012, the overall violent crime rate in the U.S. rose for the first time since 2006, and I think we should look at why and is the FBI able to work with their State and local partners in this. I know the FBI has been at the forefront in using forensic science in its investigations. It has had problems in the past with its crime lab, and I look forward to working with the FBI to develop comprehensive legislation on forensic matters.

So I thank the Director for being here, but when I thank you, Director, I also thank the hard-working men and women of the FBI. I know you are proud to serve with them. They are proud to have you leading them. And I look forward to the Director's testimony.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Senator Grassley.

**OPENING STATEMENT OF HON. CHUCK GRASSLEY, A U.S.
SENATOR FROM THE STATE OF IOWA**

Senator GRASSLEY. Director Mueller, thank you for your service as well and extending that period of time that you are willing to serve the people of this country.

Thank you, Chairman Leahy, for calling the hearing, and I welcome Director Mueller back, particularly because this is likely to be the last hearing he will appear before the Committee.

Over the past 12 years, Director Mueller has done a good job of transforming the FBI from a law enforcement agency into a national security agency. The wall between intelligence and criminal cases has come down, and the integration of law enforcement and intelligence has worked. Those fundamental changes have made the FBI stronger and more successful in stopping terrorist attacks before they occur. They have also helped strengthen the FBI when tragic events like the Boston bombing have occurred.

Cooperation between the FBI, federal agencies and partners, and State and local law enforcement has been improved. However, there are still problems with the FBI that need to be addressed, such as retaliation against those who speak out and blow the whistle on internal problems.

That said, for a second time I thank Director Mueller for his service, and I am sure that he is looking forward to much deserved time off. Unfortunately, we still do not know who will be replacing Director Mueller when he leaves. This is very concerning and, of course, raises questions about the upcoming transition.

For starters, the President has not submitted a nominee to the Senate to fill the vacancy. There have been media reports that the President intends to nominate James Comey, former Deputy Attorney General in the Bush administration, but no official nomination

has been received. It is unclear what the intention of the White House is with the release of Mr. Comey's possible nomination.

Whatever the motivation, it does not change the fact that the President has not formally nominated anyone to succeed Mueller. The President needs to send a nomination to the Senate and in short order; otherwise, we will not have enough time to properly vet the nominee and ensure that the new Director is in place prior to Director Mueller's departure. Given the FBI's role in counterterrorism, counterintelligence, and criminal law enforcement, any delay in appointing a Director means a vast bureaucracy will be left to an Acting Director.

I would like to hear from Director Mueller about the transition planning, how he intends to hand things over to the next Director, and what contingency plans are in place in the event an Acting Director is necessary.

There are a number of other matters to discuss.

First, there has been a lot of news following the classified leaks of two national security programs operated by NSA and utilized by the intelligence community. The leak of classified information related to the 215 business record program and the 702 foreign intelligence has started a debate about whether these programs strike the proper balance between civil liberties and our security. As a result of the release of information, the administration chose to release additional details explaining how the programs operate, including the facts surrounding successes in thwarting terrorist attacks.

More importantly, the information details the various safeguards and programmatic oversight built into the program. I am always of the opinion that more oversight is needed of the Federal Government, and given the classified nature of these programs, Congress needs to be extra vigilant in conducting oversight of these programs.

Yesterday's public hearing held in the House Permanent Select Committee on Intelligence was a good opportunity for Congress and the administration to show the American people that these programs can be discussed in an open manner. More hearings should be held so people better understand how the 702 program and Section 215 work. This includes the necessary declassification of information to assist Congress in determining whether the law was followed. Absent some level of transparency, the American people will not understand how their government works.

There is a lot of distrust in government these days, and it is certainly understandable given the scandal at the IRS, the secrecy surrounding the administration use of drones, subpoenas seeking reporters' emails and telephone calls, along with the effort to legislate in spite of constitutional protections and civil liberties. An open and transparent discussion of these programs is the only way that the American people will have confidence in what their government is doing.

I continue to believe that a major problem causing the leaking of classified information is the lack of whistleblower protection for members of the intelligence community. The final version of the *Whistleblower Protection Enhancement Act* that was signed into law last year failed to include protections for the intelligence commu-

nity, and I authored those. These provisions were originally included in the Senate-passed version but did not pass the House.

Specifically, it would have provided a protected method for employees to report concerns through a protected channel within the intelligence community. I believe the existence of such a channel would help stop would-be leakers from releasing classified information. So I would like to hear from Director Mueller about whether he would support such a provision.

Another critical national security issue to address is cybersecurity. The House has passed four separate bills addressing the issue. The Senate continues to address the topic in various committees. All the proposals recognize the need to strengthen the Nation's cybersecurity defenses. Where they differ is how to do it. The FBI plays a front-line role in addressing and investigating cybersecurity, so the Director might information us about what barriers exist and are preventing efforts to combat cyber attacks against our computer systems.

Regarding traditional criminal matters at the FBI, I remain concerned about the number of cases where individuals may have been convicted based on faulty FBI crime lab reports. Chairman Leahy and I sent a number of letters regarding the unpublished results of the 1996 review of the FBI crime lab. To date, we have not received a briefing on this request. The Department of Justice continues to focus only on prospective review of criminal cases and not provide answers to the Committee as to what happened during this previous review. I would like to hear what the Director says about the matter and what has been done to bring justice to defendants that may be innocent as a result of faulty crime lab work.

I will ask the Director about the FBI's plans for using unmanned aerial systems or drones. At the last oversight hearing with Attorney General Holder, I asked about the Department's use of drones, and in a written response, the Attorney General indicated DEA and ATF had purchased drones and were exploring their use in law enforcement. Absent from this response was an indication of how the FBI was using or seeking to utilize drone technology. So I will ask Director Mueller whether the FBI has purchased or is considering purchasing drones, what limitations the FBI has put in place, and how the FBI plans to use drone technology.

I will ask about the FBI's investigation into Border Patrol Agent Brian Terry's murder. It has now been 2-1/2 years since the murder. The FBI has cited the ongoing investigation as a reason for not providing information. However, at some point the FBI will have to answer questions about this matter, and it is a matter of courtesy and humanity to the family to do that.

And, finally, I remain concerned that whistleblowers at the FBI continue to face retaliation and delay in clearing their names. So I will ask the Director about the final outcome of two whistleblower cases brought by employees at the FBI that I have been tracking for years. The first is that of Agent Turner, who blew the whistle on FBI employees removing evidence from the World Trade Center site following the 9/11 attack. The second is employee Robert Kobus, who blew the whistle on time and attendance fraud at the New York City Field Office FBI. The Deputy Attorney General found Special Agent Turner was subject to adverse personnel ac-

tion. Why has the FBI appealed and fought Special Agent Turner's case for nearly a decade? And what action was taken against those persons who participated in the retaliation? And in regard to the Kobus case, what is the current status of that case? And if there has been a ruling, why has my office not been provided a copy?

So thank you very much, Director Mueller, for your service but also for helping me get to the bottom of some of these things.

Chairman LEAHY. Thank you very much.

Director Mueller, we will, of course, put your full statement in the record. As I said, this is probably your last appearance here, but you have served with distinction as only the sixth Director of the Federal Bureau of Investigation, which was a great career starting your service as a U.S. Marine in Vietnam and through to the present.

We will, of course, put your full statement in the record, but the floor is yours. Go ahead.

**STATEMENT OF HON. ROBERT S. MUELLER III, DIRECTOR,
FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT
OF JUSTICE, WASHINGTON, D.C.**

Mr. MUELLER. Well, thank you, Chairman Leahy, and good morning, and thank you for the kind comments about my wife, who deserves very much of the credit, I must say. Both she and I appreciate you thinking of her. And, Ranking Member Grassley, thank you for your comments, sir. And thank you to all for giving me the opportunity here to testify on behalf of the men and women of the FBI. And on behalf of them, let me begin by thanking you for your support of the institution over the last 11-1/2 years since September 11th. Any progress that we have made in that time frame is attributable to a number of entities, one of them being this particular Committee.

Now we live in a time of diverse and persistent threats from terrorists, spies, cyber criminals and, at the same time, we face a wide range of criminal threats, from white-collar crime to child predators. And just as our national security and criminal threats constantly evolve, so, too, must we, the FBI, evolve to counter these threats, even during a time of constrained budgets.

Today I would like to highlight several of the FBI's highest-priority national security and criminal threats, starting with terrorism. As illustrated by the recent attacks in Boston, the terrorist threat against the United States must remain our top priority.

As exhibited by many of our arrests over the past year, we face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often distinct, which makes them difficult to identify and to stop.

And at the same time, foreign terrorists still seek to strike us at home and abroad. Terrorists today operate in more places and against a wider array of targets than they did a decade ago. We have seen an increase in cooperation among terrorist groups and an evolution in their tactics and in their communications.

While core al Qaeda is weaker and more decentralized than it was 11 years ago, it remains committed to attacks against the West. And al Qaeda affiliates and surrogates, in particular al

Qaeda in the Arabian Peninsula, pose a persistent threat. And in light of recent attacks in North Africa, we must focus on emerging extremist groups capable of carrying out additional such attacks.

Turning briefly to that which was mentioned, that is, cyber, the cyber threat has evolved significantly over the past decade and cuts across all of our FBI programs. Cyber criminals have become increasingly adept at exploiting weaknesses in our computer networks, and once inside they can exfiltrate both state secrets and trade secrets. And we face persistent threats from hackers for profit, organized criminal cyber syndicates, and what we call "hacktivist groups."

As I have said in the past, I do believe that the cyber threat may well eclipse the terrorist threat in years to come. And in response, we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

The Cyber Division is focused on computer intrusions and network attacks. FBI special agents work side by side with federal, State, and local counterparts on cyber task forces in our 56 field offices, working together to detect and disrupt computer intrusions.

We have increased the size of the National Cyber Investigative Joint Task Force, which brings together 19 law enforcement, military, and intelligence agencies to stop current attacks and prevent future attacks. And cyber crime requires a global approach, and through our 64 legal attache offices overseas, we are sharing information and coordinating investigations with our counterparts.

Finally, on this particular point, we recognized that the private sector is an essential partner to protect our critical infrastructure and to share threat information. We have established several noteworthy outreach programs, but we must do more. We need to shift to a model of true collaboration, build structured partnerships within the government and in the private sector.

Turning to the FBI's criminal programs, we have a great range of responsibilities from complex white-collar fraud to transnational criminal enterprises, and from violent crime to public corruption. And given the limited resources, we must focus on those areas where we bring something unique to the table.

For example, violent crime and gang activity continue to exact a high toll on our communities and through Safe Streets and Safe Trails Task Forces, we identify and target the most dangerous of these criminal enterprises.

At the same time, the Bureau remains vigilant in its efforts to find and stop child predators. Our mission is threefold: first, to decrease the vulnerability of children to exploitation; second, to provide rapid, effectiveness response to crimes against children; and, third, to enhance the capabilities of State and local law enforcement through task force operations such as the Innocent Images Initiative and the Innocence Lost Initiative.

Now, let me pause for a second and spend a moment discussing the recent public disclosure of highly classified national security programs.

The highest priority of the intelligence community is to understand and combat threats to our national security, and we do so in full compliance with the law. We recognize that the American pub-

lic expects the FBI and the intelligence community to protect privacy interests, even as we must conduct our national security mission.

The FISA Court has approved both programs, and these programs have been conducted consistent with the Constitution and the laws of the United States. The programs, as we heard yesterday, have been carried out with extensive oversight from the courts, from Congress, and from independent Inspectors General. And these programs do remain classified, so there are significant limits on what we can discuss this morning in an open session.

I do know that there have been classified briefings on these programs for Senate Members over the last couple of weeks, and I hope most of you, if not all of you, were able to attend. And if you were unable to, I would suggest and encourage you to do so.

As to the person who has admitted to making these disclosures, he is the subject of an ongoing criminal investigation. These disclosures have caused significant harm to our Nation and to our safety, and we are taking all necessary steps to hold accountable that person responsible for these disclosures. But as this is a matter actively under investigation, I cannot comment publicly on any of the details of the investigation.

Now, in closing, I would like to turn to sequestration. The impact of sequestration on the FBI's ability to protect the Nation from terrorism and crime will be significant. In Fiscal Year 2013, the FBI's budget was cut by more than \$550 million due to sequestration. In Fiscal Year 2014, proposed cuts will total more than \$700 million. The ongoing hiring freeze will result in 2,200 vacancies at the FBI by the end of this Fiscal Year with another 1,300 additional vacancies in 2014.

I have said and you have said that the Bureau's great asset are our people. Additional operational cuts will impact our ability as an organization to prevent crime and terrorism, which will impact the safety and the security of our Nation.

I will say we all understand the need for budget reductions, and we are going through a thorough review of every dollar spent, and I am sure we can find savings. I would like to work with the Committee to mitigate the most significant impacts of the cuts, both this Fiscal Year and those we anticipate for the next fiscal year.

Chairman Leahy, Ranking Member Grassley, and Members of the Committee, I again would like to thank you on behalf of the Bureau and all our people for your support of the FBI and its mission. Our transformation over the past decade would not have been possible without your cooperation. Again, thank you personally and on behalf of the FBI for your efforts and your contributions, and I look forward to answering any questions you might have.

[The prepared statement of Mr. Mueller appears as a submission for the record.]

Chairman LEAHY. Well, thank you very much, Director, and I share your concern about sequestration. The kind of meat axe approach of that has been devastating to law enforcement. It has been devastating to some of the critical work we do in seeking cures for major diseases. In a number of areas, it has put out scientific efforts behind so many other countries, and it is questionable whether it will take us decades to get caught back up.

Let me talk about the PATRIOT and FISA authorities. As you know, I have had concerns about Section 215 of the *PATRIOT Act* and Section 702 of the *FISA Act*, the Foreign Intelligence Surveillance Act, for a number of years.

Now, the Director of National Intelligence has declassified some more information about the bulk collection, the huge amount of collection of phone records under Section 215, and I think the American people want to know if it has been sufficiently effective to justify what is a very expansive scope.

Last week, I asked the Director of the National Security Agency, General Alexander, to provide specific information—he had been going in broad generalities. I asked him for specific information about cases where data obtained through Section 215 proved critical to thwarting a terrorist threat, even if he had to do it in a classified setting. He promised he would provide that by now, by this time this week, and he has not yet, but I assume that having promised publicly that he would, he will.

Last week, we heard it was dozens of plots. Yesterday we heard it was 50. But then either way, it seemed clear that the majority of those cases were not under Section 215. They were 702, an entirely different type of program.

So let me ask you this: Have phone records obtained through Section 215 of the *PATRIOT Act* been critical to the disruption and discovery of terrorist threats? And if so, how many times?

Mr. MUELLER. Well, the answer to that is yes. I would say for most of the occasions it has been a contributing factor, one dot amongst a number of dots, but there are those cases where it has been instrumental. The one that was mentioned yesterday is an individual out of San Diego who we had opened in 2003, based on an anonymous tip that this individual was involved with Al-Shabaab, providing support to Al-Shabaab in Somalia. We did an investigation. We closed the investigation down.

Chairman LEAHY. But in that case, the initial was from a tip, not from something—

Mr. MUELLER. That was in 2003. We closed it down in 2003. In 2007, NSA was up on a telephone line in East Africa. They had the number of that telephone line, but they could not tell what calls were made to that telephone line in East Africa. And, consequently, they took that number, ran it against a database, and came up with this number, telephone number in San Diego. All they had was a number. They then go through the additional legal process to get the subscriber information that is not included in the database, and from that went up on a *FISA* after they gained the requisite predication. That was a case that was solely based initially—the reopening of that case, that person has been convicted, I think pled guilty, and is about to be sentenced. But that is one case where you have 215 standing by itself.

Now, the point—

Chairman LEAHY. Is it possible to say how many where 215 has been critical? Because we are talking about billions of phone numbers. How many—

Mr. MUELLER. Let me, if I could, say two things. You are going to get—I know we are working through the list of numbers—or not numbers, the list of cases, and of those domestically I think there

will be anywhere from 10 or 12 where 215 was important in some way, shape, or form.

Chairman LEAHY. Out of the billions of phone numbers that were collected.

Mr. MUELLER. Yes, but let me go back to September 11th. On September 11th, al-Mihdhar was one of the principal hijackers ultimately—I think he was in the plane that—one of the planes in New York, but I may be wrong on that. But he was a principal hijacker, and the intelligence agencies were on him, tracking him through the Far East. Nobody had him in the United States. Ultimately he comes to the United States in 2000.

Sometime thereafter, the intelligence communities are on a number in Yemen that is known to be affiliated with terrorists. At that point in time, without this particular capability, they had no way of identifying whether there was somebody in San Diego calling this number in Yemen. The IG report afterwards indicated that had we had this information, we may well have been able to stop the attack. If we had had this program in place then, the NSA or the intelligence community would bring that number to us, we would run it against that database, and what would come up was Mihdhar's number in San Diego, and we go through exactly the same routine we did—

Chairman LEAHY. I understand, but you also have a whole lot of other things that happened there. I mean, the 9/11 Commission showed that the failure of the CIA and the FBI—and I realize it was before your time, but the failure of the CIA and the FBI to share information created problems. Al-Mihdhar had been placed in the State Department's tip-off watchlist. Had the CIA shared records with the FBI, that might have made a difference.

Had Minnesota had the warnings—

Mr. MUELLER. Moussaoui.

Chairman LEAHY. Had the warnings of the agent out there been followed up in Washington, that might have made a difference. We could look at a whole lot of things that I assume we are doing a lot better today. But the—and, of course, we know that the President was told in August of a serious concern about this.

So I realize the mistakes were made before 9/11. We are trying to close that. I just want to make sure if we are collecting—I was concerned about the testimony last week by the NSA as though somehow—and they were conflating 215 and 702 as though this was critical to everything, and yet as you know, you collect several billion phone calls, and sometimes you do not have anything unless you got a tip from just good police work that makes you look back and find out what those—what numbers are worthwhile.

I worry that we get so imbued with the technology that we forget that somehow all the technology in the world does not begin to help as much as just collecting the dots, connecting the dots.

Mr. MUELLER. Well, I think what concerns me is you never know which dot is going to be key. What you want is as many dots as you can. If you close down a program like this, you are removing dots from the playing field.

Now, you know, it may make that decision that it is not worth it, but let there be no mistake about it, there will be that fewer—those fewer dots out there to connect if you do not have that ability

to go back in records that retain the toll records or a database that retains those toll records and identify that particular person in the United States who is in communication with the terrorist number overseas.

Chairman LEAHY. I will have further questions, but one of them I have again on connecting the dots, we have heard conflicting testimony that on the Boston Marathon bombing, even though the Boston police had four officers assigned to the Joint Terrorism Task Force, they were not given all the information the FBI had about what the Russian security service said, cryptic though it might be, and were not told that Tamerlan intended to travel abroad. Is that true?

Mr. MUELLER. Well, yes and no. Let me, if I can explain. It is a Boston task force. The Boston task force last year had probably close to 1,000 threats related to counterterrorism. You do not—everybody on that task force handles federal threats or local threats or what have you. It is a task force. The question, I think, from Ed Davis' point of view is, should the hierarchy of the Boston Police Department have been informed?

This, because it was resolved, it was not an immediate threat, did not get briefed up through the task force to the higher levels of the FBI, much less the other participants in the task force. So I do not think it is fair to criticize the task force concept for not—in something like this, doing the briefings higher up the chain of command given the number of cases that we handle in this area.

I will tell you that if you talk to State and local law enforcement, I think they will say that the work that we did in the course of this investigation was first rate, that the relationships that we have developed over a period of time are extensive, and the success of bringing—identifying the two who were responsible for it in such a short period of time is attributable to that work of State and local law enforcement, but also contributed to by us and the relationships.

Chairman LEAHY. Thank you very much. And I apologize to Senator Grassley for taking extra time on this, but please go ahead.

Senator GRASSLEY. I just told him he does not need to apologize. He is Chairman of the Committee.

During the last hearing, May 2012, Senator Hatch asked a question as to whether or not President Obama discussed potential successors with you. You responded at that time that he had not in the past—or he had in the past but not recently. Now, I do not expect to get any information on the content of a discussion you might have with the President, but I do ask this question: Since the hearing, May 2012, have you discussed potential successors with President Obama?

Mr. MUELLER. Well, yes. I generally do not like to get into conversations between myself and—

Senator GRASSLEY. No, and you—

Mr. MUELLER. But I will say yes, without any of the content.

Senator GRASSLEY. You have answered the question.

Mr. MUELLER. Okay.

Senator GRASSLEY. Do you have a transition plan in place for your successor? And if so, how much time is needed to implement the plan in order to provide a seamless transition?

Mr. MUELLER. We have been preparing, as you can imagine, for the last two years—in fact, the last two and a half years, and we have already prepared the extensive materials that the successor will have to review. We are prepared to start the briefings as soon as the person is sworn in. We have been looking at personnel so that there can be some overlap of personnel so that the person comes in and has key components that are ready to support them, in the same way that when I came in before September 11th, the FBI supported me.

Senator GRASSLEY. Approximately how much time is necessary for that?

Mr. MUELLER. Well, it is a learning experience, and we will get the briefings and the like, but it will take maybe three—I would say a month to really get one's feet on the ground. But in that month, I can tell you something is going to happen, so whatever you planned in terms of sitting down and looking at something, something else will come up, and your attention will be diverted. So it is hard to say a specific time frame.

Senator GRASSLEY. This is so important because we will have about four weeks in July, we will have only four days after your term ends to consider a nominee.

Do you have any idea when we might expect a nominee to come up from the White House?

Mr. MUELLER. I do, but I am not in a position to be able to advise the Committee.

Senator GRASSLEY. Okay. Then let me go on to another one. This involves Fast and Furious. In my opening statement, I said I know that the FBI does not talk about ongoing investigations. However, eventually the FBI has to talk about the Brian Terry murder investigation, just like eventually you had to talk about the anthrax investigation.

I am going to be submitting a detailed list of questions about the concern that the Terry family has that there was an attempt to cover up the connection between the guns and the ATF operation. According to the family, the indications of an attempted coverup have not been fully investigated.

So all I am asking you now: Would you be able to respond to my written questions before you leave office?

Mr. MUELLER. I would have to look at it and see how extensive, but we will make every effort to do so.

Senator GRASSLEY. Okay. And then just one question in regard to this issue, so I will ask right now. On October 20, 2011, I wrote you to ask what time the FBI arrived in Peck Canyon where Border Patrol Agent Brian Terry was murdered. There are conspiracy theories out there that the FBI or an FBI informant was out in Peck Canyon before Agent Terry was shot. Do you believe that there is any truths to those theories?

Mr. MUELLER. No, I do not believe there is any truth in those theories, but I would have to go back and make certain. Off the top of my head, I do not believe there is any truth, but I would like to go back and make certain that we have nothing that would be supportive of those theories.

Senator GRASSLEY. Okay. And then I would like to have that in writing.

Senator GRASSLEY. I want to go to drones. In recent responses to questions I asked Attorney General Holder following his last oversight hearing, the Department of Justice advised this Committee that both DEA and ATF have acquired unmanned aircraft systems. The Department indicated that those agencies were drawing up plans and procedures to use them. The responses did not indicate whether the FBI had acquired any drones and whether there were future plans for drone technology use by your agency.

Does the FBI own or currently use drones? And if so, for what purpose?

Mr. MUELLER. Yes, and for surveillance.

Senator GRASSLEY. Okay. Does the FBI have any agreement with any other government agencies—let me suggest a couple; there might be others: DOD and Homeland Security—to receive assistance in the use of drones?

Mr. MUELLER. I am not certain. I do not think so. But whenever—well, all I am saying is that one of the issues with drones, any use of drones by any agency, is what happens in the airspace. To the extent that relates to the airspace, there will be some communication back and forth.

Senator GRASSLEY. So instead of asking you a question, I think I can assume, since you do use drones, that the FBI has developed a set of policies, procedures, and operational limits on the use of drones, and whether or not any privacy impact on American citizens.

Mr. MUELLER. We are in the initial stages of doing that, and I will tell you that our footprint is very small. We have very few, and of limited use, and we are exploring not only the use but also the necessary guidelines for that use.

Senator GRASSLEY. Does the FBI use drones for surveillance on U.S. soil?

Mr. MUELLER. Yes.

Senator GRASSLEY. I want to go on to a question—

Mr. MUELLER. Well, let me just put it in context.

Senator GRASSLEY. Sure.

Mr. MUELLER. In a very, very minimal way and very seldom.

Senator GRASSLEY. Okay. Currently it is a crime to purchase material for the production of illegal passports, to forge illegal passports, to distribute illegal passports, and to engage in other criminal activity that facilitates trafficking of false passports. The immigration bill before the Senate will weaken this current law. Under the bill, only those who produce, issue, or distribute three or more passports will have committed a crime. Under the bill, only those who forge, alter, or possess or use three or more passports will have committed a crime. Even more outrageous under the bill, only those who use any official material to make 10 or more passports will have committed a crime.

Question: Will these changes in current law have a negative impact on counterterrorism or counterintelligence efforts of the FBI?

Mr. MUELLER. I am not familiar with the current law, and even less so with the proposed law, so I would have to get back to you on that particular question.

Senator GRASSLEY. It would be very important that you get back to us in two or three days, because these are issues before Congress right now.

Mr. MUELLER. I will try to, but I must say I am not certain we have that much experience in the prosecution under those statutes. But let me look at it, and we will try to get back to you in short order.

[The information referred to appears as a submission for the record.]

Senator GRASSLEY. Would you agree with this, that the weakening of current law creates a loophole that could allow terrorist groups such as al Qaeda or Hezbollah or other foreign spies to more easily operate within the United States?

Mr. MUELLER. Without analyzing the bill, I really am not in a position to opine on it.

Senator GRASSLEY. Okay. I will yield.

Chairman LEAHY. Thank you very much.

Senator Feinstein.

Senator FEINSTEIN. Well, thank you very much, Mr. Chairman. You made several remarks as to the integrity and the service of the man before us. I cannot help but note it is the first time I have seen just one person at this very long table. I think that is due deference.

Director Mueller, I first met you when I was mayor—and I think it was 30 years ago—and you were United States Attorney in San Francisco. I have watched your progress. I have watched you serve two Presidents, one Republican, one Democrat. I have watched your extraordinary integrity. I have watched you remove the FBI from certain interrogation having to do with detainees when you did not think it was appropriate. I consider you to be a man of high integrity and very strong values, and I think that you have brought that also and strengthened it in the organization you represent.

I for one, and I think everyone, am very sad to see you go. You look young and vital to me, and—

Mr. MUELLER. I feel that way, too, I might add.

Senator FEINSTEIN. Well, that is good. I wanted to just have a talk with you about these two programs, because I go front and center with them as Chair of the Intelligence Committee of the Senate. And, you know, we have looked and tried to provide the oversight and see that they follow law. We had a classified briefing—and I will say one thing about it—for 47 members and had the former chief judge of the Foreign Intelligence Surveillance Court there to explain how the Court proceeds.

I, as you do, believe that both these programs are legal, that they are carefully overseen. Senator Leahy mentioned the one that collects phone record data, not the names but the data, not the content but the data. Only 22 people have access to it, and it was queried approximately 300 times only this past year.

You yourself mentioned that it was responsible and helped in 10 to 12 percent of the 50 cases where the NSA has said it is helpful. I am asking you now for a qualitative judgment. I have made mine. How do you judge the 10 to 12 percent: as highly worth it or not worth it?

Mr. MUELLER. I think it is very difficult to judge a program in that particular way, particularly a program that will give you a key to preventing a terrorist attack. And how that one lead you have, how can you differentiate that from five or six or others that may come up in the same place? Which of those leads is going to be the one to help you disrupt a plot?

In my mind, the communications capabilities of terrorists is the weakest link. If we are to prevent terrorist attacks, we have to know and be in their communications. Having the ability to identify a person in the United States, one telephone number with a telephone that the intelligence community is on in Yemen or Somalia or Pakistan or what have you may prevent that one attack, that Boston or that 9/11. And so, on the one hand, yes, it is relevant evidence; yes, it is critically important that we have that link. And then the question is: When you legislate it and you have this vast volume of records, how do you appropriately give oversight at the Justice Department in the National Security Division, in the Inspector General's office, through the *FISA* Court, and through Congress. And I think anybody who looks at these programs wants to make sure they are legal, that they are effective, that there is appropriate oversight because it does raise national security and civil liberties concerns.

But once you look at that, once you identify it, then are you going to take the dots off the table, make them unavailable to you when you are trying to prevent the next terrorist attack? That is a question for Congress.

Senator FEINSTEIN. Well, the way I looked at it, particularly with Nazibullah Zazi, was that this was an attack which could have killed hundreds if not thousands of people, that he was not going to be the lone perpetrator, that we know there were at least two conspirators who were going to participate in it. We know about other things that showed that there were going to be more people. And it seems to me that if we were not able to protect it and the New York subway were blown up in a number of different places, with hundreds of people or thousands of people literally being killed, that there would be no question as to its value and worth.

I have come to believe that the only way we prevent these attacks is good intelligence. How do you get good intelligence when likely one of the conspirators is in another country, connected with a terrorist group, and one is in this country prepared to carry it out? So to me, the value of those programs in preventing loss of life in this country is substantial.

Here is the question. Because you have that 10 to 12 percent, do you think it would be possible not to collect the database but to be able to query the database if the time for keeping that database was extended to five years with the phone companies?

Mr. MUELLER. I know Keith Alexander and others are looking at the possibility of restructuring the program in this way. In my mind there are two disadvantages—maybe three.

First of all, there is no records retention requirement on telephone companies at this point, and they are all over the lot. Some may do it—and I throw this out—18 months, some may be less, some may be more. And in that database that they keep will be those numbers that are calling the suspect numbers overseas.

Second, if you have a number in Yemen, that would require you to go to three or four or five or six particular carriers with separate legal paper and require them to come and pick up what they have collected and are keeping there and get back to you—the point being it will take an awfully long time. And in this particular area, when you are trying to prevent terrorist attacks, what you want is that information as to whether or not that number in Yemen is in contact with somebody in the United States almost instantaneously so you can prevent that attack. You cannot wait three months, six months, a year, to get that information and be able to collate it and put it together. Those are the concerns I have about an alternative way of handling this.

Senator FEINSTEIN. Well, let me ask you this: Is it 10 or 12 cases or 10 or 12 percent?

Mr. MUELLER. Ten or 12 cases. I should have—

Senator FEINSTEIN. Ten or 12 cases.

Mr. MUELLER. Yes, and some of them are two—I am not certain whether all of them are 215. They are a combination or one or the other.

Senator FEINSTEIN. I see. Thank you.

One other quick question. People are concerned about privacy. I think the greatest threat to the privacy of Americans is the drone and the use of the drone and the very few regulations that are on it today and the booming industry of commercial drones.

You mentioned that you use it for surveillance. What are the privacy strictures on the use of drones by your agency today?

Mr. MUELLER. Well, it is very seldom used and generally used in a particular incident where you need the capability. I will have to go back and check in terms of what we keep in terms of the images and the like. But it is very narrowly focused on particularized cases and particularized needs in particularized cases, and that is the principal privacy limitations we have.

Senator FEINSTEIN. I would like to get that information. I think it would be helpful to us legislatively.

Mr. MUELLER. I will be happy to do that.

Senator FEINSTEIN. Thank you very much.

Senator FEINSTEIN [presiding]. Senator Hatch, you are next.

Senator HATCH. Well, thank you so much, Madam Chairman.

Well, I came here today basically to thank you for your service. I also want to thank Senator Feinstein for her kind remarks about you. Senator Feinstein has done an excellent job on the Intelligence Committee. Up until I left a few years ago, I believe I was the longest-serving person in history on the Intelligence Committee, so I have been fully aware of these matters. And all I can say is I want to pay tribute to you, General Alexander, and others in the intelligence community and the FBI for the work that you have done to protect our country and to ferret out these problems that really could have been very disastrous had we not had the abilities that you have been describing here today.

But I also want to personally thank you for the terrific service you have given. I have watched you very carefully. I have been Chairman on this Committee. I have been Ranking Member on this Committee. I just have to say that I do not know that we have ever had an FBI Director as good as you are, and, frankly, every one

of us has confidence in you and your ability and your integrity. That is a pretty high comment, really, because we—and that is meant very, very sincerely. I have watched you over the years. I have watched the FBI do the job that in many ways they never get thanked for and really are not—in many ways people do not even know about it. It is a thankless job in many ways, and you have given almost 12 years of your life to this type of work. I just want to personally tell you how much I personally appreciate you and appreciate the FBI and those who have served with you all these years. And I wish you the very, very best when you finally do hang them up here, and I think all of us—or at least I can speak for most all of us, we just think you are terrific.

I will not take any more time, but I just wanted to make sure I let you know just how deeply I feel toward you and those at the FBI who have been doing such a great job all these years.

Mr. MUELLER. Well, thank you very much, Senator. I remember you chaired my confirmation hearing—I will not forget that—a number of years ago. But I have been very lucky and fortunate to have the opportunity to do this job, which I have loved and enjoyed, and thank you for those comments.

Senator HATCH. Well, you have done a great job. Thank you.

Senator FEINSTEIN. Thank you very much, Senator Hatch.

Senator Klobuchar is next. I do not see her. Senator Franken is not here. Senator Sessions.

Senator SESSIONS. Well, those were kind comments, Director Mueller, and I would echo them. You know my admiration for you as a professional is exceedingly high, and you came to the office with the kind of skills, experiences that others have noted that gave you an opportunity to be very, very effective in this important position. So I really salute you for that. Your integrity is undoubtedly, and your experience and love of your country is undoubtedly. So I wanted to join in my comments in that regard.

There are so many things that are happening now, and I think the FBI needs to rise to the occasion. The FBI is such a premier investigative agency. I had the honor to prosecute cases brought to me by FBI agents for almost 15 years, and I met with them personally for hours and weekends and nights and know how meticulously they work to do everything exactly right. And when I hear people have doubts, great doubts sometimes, about the integrity of the average cases and agents that I know, I know that is just not right. They try to do the right thing every day. If they are involved in anything seriously wrong, discipline will fall swift on them. They can make mistakes, and Congress sometimes creates circumstances that puts them in difficult positions, and life is tough for agents out there. But, fundamentally, day after day, I have worked with FBI agents. They are personal friends of mine, remain so for decades, and I just want to share those thoughts.

Maybe you would like to comment about the fidelity of your agents.

Mr. MUELLER. You are not going to find a better group of people to serve with. The testimony was most firmly felt when I was a new person in the institution. In the wake of September 11th and the organization, every agent, every analyst, every professional support staff worked flawlessly in response to that. And that was

just indicative of the capabilities of the organization and the quality of the people.

Senator SESSIONS. Well, I agree. Director Mueller, one of the big matters before the Nation today is the IRS scandal involving the actions that have been taken to target conservatives or Tea Party groups. It so happens that I know Becky Gerritson of the Wetumpka Tea Party, who testified before the House Committee. And she was a normal housewife, American citizen, who got deeply engaged in trying to make her country better. She loves this country. Her integrity is high. She was trying to do the right thing. And I believe that the IRS did not perform and handle their applications for status correctly. I believe it is a very serious matter, and I am concerned about it.

You were asked last week, I believe, about this as to whether or not the victims, the potential victims of these abuses have been interviewed, and I believe you said no. I believe on May 14th Attorney General Holder said that an investigation had been commenced. Is the FBI the lead agency of the IRS matter?

Mr. MUELLER. Yes.

Senator SESSIONS. And you have designated agents in charge of that investigation?

Mr. MUELLER. Yes, I have.

Senator SESSIONS. And you were asked before whether you knew the names of those. Can you tell us those names or how many have been assigned to it?

Mr. MUELLER. I can say that over a dozen agents have been assigned locally. I can tell you that it falls within the purview of Valerie Parlave, who is the Assistant Director in charge of our Washington office, who is in charge of this investigation at the field level; but we also have people at headquarters that are monitoring it.

I cannot tell you who in the course of the investigation has been interviewed. I will tell you that before we initiated the investigation, if—and we did get complaints, those individuals were interviewed before we even initiated an investigation. And they would be the victims which you mentioned.

Senator SESSIONS. Well, the FBI is the right agency, in my opinion, without question. It should not be the internal IRS IG or others. And you have the independence to do that effectively, and I believe you can do that. But I called Ms. Gerritson this morning. It so happens she was discussing with a lawyer, and they said they have been talking to other so-called potential victims, and none of them have been interviewed, none of them have been contacted about an interview, even an appointment set up with them. I think that is pretty slow. I think the first thing you do from my experience is you go out and interview the people and find out what conversations they had, what documents they have, what the basis parameters of the problems are, and get busy on it.

Do you think—it seems to me that you are running behind here. What would you say about that?

Mr. MUELLER. Well, I am not familiar with the day-in and day-out details of the investigation. Quite obviously, given what you have said, I will go back and see where that is. But also in these investigations, one of the first things you do, as you well know, as

a prosecutor is have the records so that when you do the interviews you have the requisite materials so that you can do an effective interview.

Now, I am hypothesizing because I do not know what is happening at the level of who in particular is being interviewed. But I will go back and check on that.

Senator SESSIONS. I think you need to get that level. I think it is too slow. And I think you can always have agents, well, we are getting our records together, and we are reviewing some—

Mr. MUELLER. No, I understand that.

Senator SESSIONS. Somebody needs to go out and find out what the problem is, talk to the people and see what the problem is first.

Mr. MUELLER. I tell you, there is urgency with the investigation. It is not languishing.

Senator SESSIONS. All right. And I would share with Senator Grassley deep concern that this immigration bill would say for passports, which you should be aware of and they need to be on top of, only those who produce, issue, or distribute three or more passports have committed a crime. Under the bill, only those who forge, alter, and possess three or more passports will have committed a crime. And only those who use any official material to make 10 or more passports will have committed a crime.

So I hope you will look at that. We would like the FBI's advice if this makes it more difficult to produce integrity in the passport processing business. Would you look at that?

Mr. MUELLER. Yes, will do.

Senator SESSIONS. Thank you.

Mr. MUELLER. Yes, will do.

Chairman LEAHY [presiding]. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you so much, Director Mueller. Thank you for your wonderful service for the last 12 years. Thank you for the work that you have done in Minnesota. And I think the Nation was riveted with the work that you did and your agents did with Boston, so thank you for that. And I also noticed there were ATF agents there, so I am going to start with that.

We just had a hearing for the President's nominee for the head of the ATF. Do you think it would be helpful to have a permanent head of the ATF?

Mr. MUELLER. I think it is always beneficial for the agency to have a permanent head.

Senator KLOBUCHAR. Very good. Are you aware that since the position became confirmable that this Congress has not ever confirmed anyone for the job?

Mr. MUELLER. I understand that.

Senator KLOBUCHAR. Yes. And one of the ideas put out there, if they are just simply not going to or are unable to get bipartisan support for a nominee, enough, at least, to put us over the top so we get a confirmed nominee, is Senator Durbin's idea to actually put the ATF under the FBI if for a number of years it goes without getting a confirmed Director. What would you think of that idea?

Mr. MUELLER. That is something that would require a great deal of study before one wanted to embark on some sort of merger.

Senator KLOBUCHAR. I understand. I just think we are at the point where we have 2,400 agents who deserve a permanent head, and just as your agents have a permanent head, and I am hopeful we will be able to get this done this year. But I just wanted to put that out there for your people to think about because we are sort of left with, we hope, a confirmation ahead. But if that does not happen, we have to think of other ways to get this done. So I appreciate that.

The other question—there have been several questions on the NSA issue, and I appreciated your comments earlier, I think it was to Chairman Leahy, about supporting declassifying, or working to do that, some of the *FISA* opinions. Is that correct?

Mr. MUELLER. Well, I have not been asked about the *FISA* opinions in particular. What we were talking about was the examples of where either 215 or 702 had been used. My understanding, though, is that the ODNI is looking at declassification possibilities with regard to the *FISA* Court orders, if that is what you are—

Senator KLOBUCHAR. Yes, that is what I meant.

Mr. MUELLER. Yes.

Senator KLOBUCHAR. And so do you think that could work?

Mr. MUELLER. I leave that—there was testimony in yesterday's hearing before the House with regard to that ongoing process, and I would have to defer to the ODNI for an answer on that.

Senator KLOBUCHAR. I appreciate that, and I also appreciate the information that has been put out to show the number of terrorist attacks that have been averted. I think that is important for the public to understand exactly what is going here and get the facts right about the numbers.

Can you talk about—and maybe you want to defer this to another time—the various checks throughout the process for data collection and analysis that people would understand would protect privacy?

Mr. MUELLER. Well, certainly if you look at 215, the significant figures, you do have a database. It just has metadata in it, numbers, it does not have any information with regard to who. It has those particular numbers, no content. You have just 22 persons who have access to this, to run the name—not the names, but run the numbers against the database, 20 analysts and two supervisors. And last year, there were only 300 inquiries, approximately 300 inquiries made into that database.

You then have overlapping and the overlay of oversight from the Department of Justice, the IG's office, the *FISA* Court that renews 215 every 90 days, and then, finally, the oversight from Congress. So each of the three branches of government have a role in assuring that privacy interests are protected here.

And at the other end, you have the possibility, the strong possibility and the actuality that in some cases this has been instrumental in contributing to the prevention of terrorist attacks.

Senator KLOBUCHAR. Thank you very much.

Another issue we have talked about before is the problem of synthetic drugs. We have had deaths in Minnesota as they have had in many other States, a huge increase in the number of calls to the Poison Control line and others. And as you know, we passed some legislation targeting certain of these synthetic drugs, but I believe

there is still more work to be done, and I am working on the so-called analog drug provision where I think that we could do more with that. But could you update us on the general state of synthetic drug use in the U.S. and how the provisions we passed last year are helpful and what more you think we could do?

Mr. MUELLER. Well, I am somewhat familiar with that, know it is on the increase. I am not familiar with the last part of your question as to what more we could do. It is really not our bailiwick. It is more DEA. And particularly in the time of budget constraints where we have to prioritize, that unfortunately drops down further on our list.

Senator KLOBUCHAR. Right, and we have been working with—

Mr. MUELLER. We are sympathetic and supportive, but I wish I could do more.

Senator KLOBUCHAR. Right. We have been working with DEA on this issue. It is just that I continue to see that has not gone away, and it obviously contributes to other crime as well. So I just want to put it on your radar screen.

We are working on a bill on metal theft. We have seen a lot of that throughout the country with buildings and issues, and I know you talked about high-tech stalkings, the cyber crime issue. And you have said you believe the FBI must change with evolving technology to better address criminal and national security threats. What is the FBI currently doing to keep up with the changes in technology?

Mr. MUELLER. Well, internally, let me just say we understand that we have to have the basic knowledge of technology to conduct investigations in this age. Every agent, to the extent that you need to be refreshed on where we are in order to do our job, is getting greater training.

Our specialists, we have got more than 1,000 personnel around the country that are specialists in this particular area. But I think the key for us is the NCIJTF, National Cyber Investigative Joint Task Force. Following the pattern of what we did after September 11th is understanding that we cannot do it alone. Having a task force concept where you have all of the major players in the cyber arena participating so that if there is a substantial intrusion, we immediately have those who would be involved, whether it be DHS, NSA, DOD, there trying to determine how to address it is critically important.

The other thing that we have done and put a great deal of focus on in the last six to eight months is work with private industry, providing information to private industry based on what we have found so that they can protect their networks. So growing internally, growing the NCIJTF, and then building our capacity with the private sector have been the three areas that we have been focused on.

Senator KLOBUCHAR. Okay. Thank you very much, and thank you again for your service.

Mr. MUELLER. Thank you, ma'am.

Senator FEINSTEIN [presiding]. Thank you, Senator Klobuchar.

Senator Cruz.

Senator CRUZ. Thank you, Madam Chairman.

Director Mueller, it is good to see you.

Mr. MUELLER. Sir.

Senator CRUZ. Welcome. Thank you for testifying. You and I have known each other a long time. A dozen years ago, you were my boss at the Department of Justice, although let me say any mistakes I may make, you will be fully held harmless.

[Laughter.]

Mr. MUELLER. You were clean. Not to worry.

Senator CRUZ. Well, and let me also echo the comments of colleagues of mine on both sides of the aisle thanking you for your service and your integrity. You have spent many decades in public service focused on law enforcement, and indeed, I recall when we were working together at the Department of Justice, almost every day in the morning at staff meeting, the question you would ask was essentially: Are we locking up bad guys? And I appreciate that focus to protecting the innocent and to going after bad guys, and thank you for a lifetime of service.

Mr. MUELLER. Thank you, sir.

Senator CRUZ. I want to talk about two topics that are both of significant importance. The first is the IRS, and I want to echo some of the concerns that Senator Sessions raised about the groups that we know were targeted by the IRS that are reporting that they have yet to be contacted or interviewed by the FBI.

As you know well, in any investigation that is in a highly politicized climate, that involves potentially corruption and political interference from the White House, the investigation is a perilous endeavor and an endeavor of significant importance to the populace. And so I want to ask: What level of priority would you characterize the IRS investigation at the FBI?

Mr. MUELLER. I would say it is as high priority investigation in that there are—it needs to be handled with care, but it also needs to be pushed aggressively because it is a very important case.

As I think you are aware—we have worked together—I will pull no punches in terms of where that investigation would lead. And we would go down any path that would lead to evidence on individuals, organizations, or otherwise, and we are in the process of doing that.

We have, I think, substantial numbers in terms of those who are working day in and day out on the investigation, both internally in the FBI but also with support from the Department of Justice where we need legal process.

Again, I will have to get back to you in terms of—and as I said to Senator Sessions, in terms of the pace and progress of the interviews, but I am aware of some of the goings-on in the investigation, and I do believe that we have moved it expeditiously during the period of time we have had it open, which is probably about a month now.

Senator CRUZ. How many agents or other personnel have been

Mr. MUELLER. We have approximately 12 agents here in DC that are working on it, but also agents designated around the country because of the breadth of the investigation who also will be working on it, depending on where the investigation takes us around the country.

Senator CRUZ. And I wanted to ask additionally if the scope of the investigation includes looking into whether individuals have been politically targeted. I can tell you that we are hearing more and more anecdotal reports not just of Tea Party groups or conservative groups that were delayed or targeted in (c)(4) applications, but donors who supported Governor Romney in the campaign, who supported Republicans, who found within weeks or months of their support becoming public suddenly they were targeted for audits.

Now, those are very difficult questions to answer if there is a pattern of doing so because those audits are not generally public. But do you know if the scope has included whether there was targeting of individuals for political activity by the IRS?

Mr. MUELLER. I think you can understand that because it is an ongoing investigation, I am leery about delving into it much more about what is happening in the course of the investigation. All I can do is I assure you—and you know me—we will push it wherever it goes.

Senator CRUZ. Well, I would certainly urge the FBI not to narrowly circumscribe the scope, because the last time there was an instance of an administration trying to use the IRS to target political enemies, it was the Nixon administration, and it led to grave consequences. And I think the FBI is well situated to pursue a serious, impartial, fair, and yet vigorous investigation of whatever the scope of conduct and illegal conduct may have been.

Mr. MUELLER. Okay.

Senator CRUZ. I want to talk about a second topic briefly, which is that I am concerned that this administration's priorities in the war on terror have been misallocated; that, on the one hand, the administration has been less than vigorous in protecting the civil liberties and constitutional rights of law-abiding citizens; and yet, on the other hand, the administration has been less than effective in investigating and going after real live terrorists. And a concern in particular I have is that your efforts and those of the FBI have been unduly constrained and handcuffed. And I would point to two instances: one, the Fort Hood shooting, where we had with Major Hasan considerable evidence, including his emails with Anwar al-Awlaki talking about killing other service members; the FBI was aware of that, and yet we failed to stop that terrorist attack.

Likewise, with the Boston bombing, we had considerable evidence with the Tsarnaev brothers of their affiliation with radical Islamic views, their advocacy of those views. We had reports from Russia, and yet we failed to stop that attack.

In your view, why is it that law enforcement was not able to connect the dots with Fort Hood and with Boston and prevent those attacks beforehand? And what policies have changed under the Obama administration concerning the investigation of radical Islamic terrorism?

Mr. MUELLER. Well, in neither case, whether it be Fort Hood or the Boston case, would I say that there were policies that inhibited us from doing our job. I will tell you in the Fort Hood case, prior to the time of Fort Hood al-Awlaki was seen as a proselytizer, a radical imam, but was not known to have engaged in operational activities. Consequently, when we looked at emails, we did not look

at them through the operational prism. Had we done so, perhaps other steps would have been taken.

There were judgment calls that were made in the course of that, for instance, whether you interview Hasan, that in retrospect could have gone the other way. But I do not think that there were any constraints, statutory or otherwise, that enabled us—or disabled us from doing the job.

In the case of Boston, yes, we were alerted by the Russians to Tamerlan's movement toward radicalization, and the expectation from the Russians was that he was being radicalized and would be going back to Russia to fight with perhaps the Chechens. They alerted us they wanted us to do what investigation we could and alert Tamerlan when—or alert the Russians when Tamerlan went back to Russia.

We did an investigation based on what the Russians gave us. That investigation required going through all of the databases, went to the university or the college that he attended for a period of time, interviewed his parents, interviewed him, did, I think, a very rational, responsible, and thorough investigation given the information we had.

He then goes back to Russia, and when he comes back, what we did not do, which we are going to do in the future, is the TECS alerts that come into the task force have to be identified to a particular person as opposed to just coming into a task force.

In any event, there is nothing that constrained our investigation at the outset back in 2011, and in my mind, even if we had done the one or two things that in retrospect we could have done better, I do not think we would have been able to stop that particular attack. But I do not believe we were in any way constrained from doing the investigation that we thought necessary once we had the information.

Senator CRUZ. Thank you.

Senator WHITEHOUSE [presiding]. Senator Franken, your timing is perfect. You are next in order.

Senator FRANKEN. Thank you. I apologize for—I was at a HELP Committee hearing, and I am sorry I missed—and I hope I do not ask things that have been asked before, but my staff tells me that my questions are still relevant.

First of all, I just want to thank you for your service, Mr. Director, and I believe our country is a safer place because of your steady leadership.

Mr. MUELLER. Thank you.

Senator FRANKEN. You will be missed.

I would like to turn to the subject of the surveillance programs that my other colleagues have been discussing. Mr. Director, I believe the government must give proper weight to both keeping Americans safe from terrorists and protecting Americans' privacy, and part of weighing that properly is making sure that there is enough transparency, I believe, so that Americans understand the protections that are in place.

Based on the briefings I have received, I believe these programs include reasonable safeguards, but I believe the government needs to be more transparent with the American people about these programs. And I think the American people have the right to know

what is going on, to the extent that is consistent with national security; and I believe that the government can and should provide that information, again, in a way that does not compromise our security.

Director Mueller, do you think that the government could be more transparent to the American public about these surveillance programs in a way that is consistent with national security?

Mr. MUELLER. Well, there are two levels of transparency. The first is transparency throughout the government, and transparency to certainly the *FISA* Court—it is under the *FISA* Court—and also transparency to Congress. And given the briefings and the like, I think there was transparency to those elements.

Now, when you talk about transparency to the American public, you are going to give up something. You are going to be giving signals to our adversaries as to what our capabilities are. And the more specific you get about the programs and the more specific you get about the oversight, the more specific you get about the capabilities and the successes, to that extent you have people sitting around saying, okay, now I understand what can be done with our numbers in Yemen and in the United States, and consequently I am going to find another way to communicate, and I am going to keep that in my mind. And so there is a price to be paid for that transparency.

Now, where that line is drawn in terms of identifying what our capabilities are is out of our hands. You tell us to do it one way; we will do it that way. But there is a price to be paid for that transparency.

Senator FRANKEN. And that is the question, and in order to do these programs, you need the trust of the people. And, of course, this all changes when there is a disclosure like there has been, and that is why we have obviously seen NSA be more forthcoming with that kind of transparency that I have been asking for.

I want to ask you specifically about Section 215, the authority in the *PATRIOT* Act that authorized the collection of telephone metadata. Importantly, by statute, only the FBI has the authority to request business records under Section 215. It is not the Director of National Intelligence. It is not the Attorney General. It is the Director of the FBI.

Last week, Director Clapper declassified the fact that the telephone metadata collected can be queried only when “there is a reasonable suspicion based on specific facts that the particular basis for the query is associated with a foreign terrorist organization.” He also declassified the fact that in 2012 this database was searched only 300 times.

Mr. Director, this is the kind of information that I think the American public benefits from knowing and that can build further trust between the public and the Government. Do you think that that kind of information would have compromised—would be compromising before the disclosure?

Mr. MUELLER. I certainly think it would be educating our adversaries on what our capabilities are, and the specificity that the dialogue—and you have to with the leak, because the leak looks at just a small sliver of information on a particular program. A leak does not talk about all of the oversight. A leak does not talk about

all of the legal constraints in terms of how the program operates. One has to respond, so there has to be responsive transparency in this particular instance—at this particular point in time, but, generally, no. It educates the persons, as I say, about our capabilities and makes it that much harder to prevent the next terrorist attack. And I will tell you that inevitably the communications are the soft underbelly of the terrorists. They have got to communicate. And to the extent that we can intercept those communications, to that extent we can prevent terrorist attacks. If that goes dark on us, if we are black, then we are going to be sitting waiting for the next one without the tools we need to prevent that attack.

Senator FRANKEN. I understand your view on that.

Let me ask a similar question. I have cosponsored bipartisan legislation to release, again, consistent with national security—and this is—I am asking you your judgment on this. The Court opinions interpreting key provisions in the *PATRIOT Act* and the *FISA Intelligence Surveillance Act*, I think what is hard here is that it is hard for Americans to debate the merits of a law when the law is kind of secret. Do you believe that the American people would gain trust and benefit from perhaps a redacted version of these decisions and opinions by the *FISA* Court on some of them?

Mr. MUELLER. Let me start by saying I understand the frustration. You are right, the American people are frustrated. You may be frustrated not having access to the particular legal theories espoused in those opinions.

I do know that the ODNI is looking at the possibility of releasing redacted copies. The lawyer for the ODNI spoke yesterday at the hearing and indicated that they are reviewing at least the key opinion or opinions with regard to 215 and 702 to see whether that can be accomplished. So I have to defer to the ODNI on that.

Senator FRANKEN. Okay. And, again, that is in the context of them already being disclosed, so—

Mr. MUELLER. Well, the opinions, I do not think—I do not think the opinions—maybe—

Senator FRANKEN. The opinions have not been disclosed, but the programs being disclosed.

Mr. MUELLER. Yes, yes.

Senator FRANKEN. Okay. Well, thank you again, and since this may be the last time you testify before us, I again want to thank you for your steadfast leadership and your service.

Mr. MUELLER. Thank you.

Senator FRANKEN. Thank you.

Senator WHITEHOUSE. Senator Lee.

Senator LEE. Thank you, Mr. Chairman, and thank you, Director Mueller, for joining us today and for your service to our country.

With respect to Section 215 of the *PATRIOT Act*, is it the Bureau's practice to request records or other tangible things related to Americans that themselves are not relevant to an investigation to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities?

Mr. MUELLER. I am not certain I understand the question. Are you talking—

Senator LEE. When you make a request—

Mr. MUELLER. The applicants on 215 orders, but—

Senator LEE. I understand. You are the applicants, and when you make the application, is it your practice to request things that themselves are not relevant to the investigation? In other words, do you confine your requests to those things that are related to an investigation, or are they broader than that?

Mr. MUELLER. Well, in the 215 context, the application to the Court and the Court's finding defines relevance in that particular context, and as we have talked about and as has been discussed for the last two weeks. And so I would have to direct you to the orders and the—I know that they are not published, but the fact that the *FISA* Court has ruled that the gathering of the metadata satisfies the relevance definition within the *FISA* statute.

Senator LEE. Right, right. And so with that understanding that you necessarily do cover a lot of data that is itself not closely tied to an investigation, you can understand why a lot of people would be concerned and why they would also have additional concerns about the fact that we have got not only secret data-gathering activities going on but also that they are undertaken pursuant to secret law, secret orders that the American people cannot have access to.

But if, as we have been told, it is necessary for the government to collect and store really vast quantities of information, including information on Americans that is itself unrelated to foreign intelligence or terrorism investigations, then—

Mr. MUELLER. If I may interrupt, are you talking about the metadata?

Senator LEE. Yes.

Mr. MUELLER. The telephone numbers? I want to make certain we are talking about that, not content.

Senator LEE. Yes. Yes, for now we are talking about the metadata. A lot of people have concerns about what, if any, limiting principles there are that would prevent the government from ultimately storing all information about all Americans, meaning just collecting more and more of this metadata and holding it for very long periods of time or perhaps at some point in perpetuity.

Does the Department of Justice or does the FBI have a view on the constitutionality of gathering information on Americans and storing it so long as it does not perform queries on that information?

Mr. MUELLER. I think I understand the broader question. I would say that the Justice Department believes that the program in place, 215 program, that has been upheld by the *FISA* Court is certainly constitutional. I would limit it to that set of facts because they are a discrete set of facts that with the attendant protections on privacy, that I think the Department of Justice as well as the *FISA* court believe absolutely it is constitutional.

Senator LEE. And at some point, do you sympathize with those who would say even if this is metadata, the fact that you can collect that quantity of metadata, store it for a long period of time, and the fact that it can later be searched causes—brings about a certain intrusion on privacy, even if it is a privacy intrusion perhaps not cognizable in court?

Mr. MUELLER. Well, as you well know better than most, in *Smith v. Maryland* it is not protected by the Fourth Amendment. So, yes,

sir, without a question about privacy concerns, but I would say they are de minimis privacy concerns compared to just about every other intrusion, as you get more predication in an investigation. In fact, it is at the bottom level. Do I think that it would be concerning to people to know that there is a database? Absolutely, which is why I do believe that it is important that this is upheld by not just the Department of Justice, not necessarily just by the Inspectors General, but also by the *FISA* Court and Congress.

Senator LEE. Okay. And, you know, I think it is important to remember also that the precedent you cited is, of course, decades old and it did not deal with the sheer volume of metadata that we are now talking about. The technologies that are at issue now did not exist then, certainly were not even contemplated then. And the more you aggregate large quantities of metadata, potentially on every single American citizen, and you give someone within the executive branch of government the power to search all of that, you do give them a pretty broad view into the lives of the American people. The more data you get, the more you add to that metadata, even if any one of those data points might be itself constitutionally insignificant, don't you think you start to approximate a point at which you start to breach a reasonable expectation of privacy?

Mr. MUELLER. I certainly believe that there quite probably is a scale, yes, but it was the same dialogue we had 20, 30 years ago about telephone toll records which triggered the *Smith v. Maryland* case. And it is the same debate, albeit with metadata as opposed to telephone toll records, but you have pretty much the same piece of data in both cases. So I would argue that *Smith*, even though it is not exactly the same as a telephone toll record, the proposition that was espoused by the Supreme Court in *Smith v. Maryland*, is applicable today. The comparable—

Senator LEE. Did we have—

Mr. MUELLER. The comparable data, let me just put it that way.

Senator LEE. Right. Did we have the capacity to gather, analyze, and store in perpetuity that kind of metadata on every single American citizen at that point?

Mr. MUELLER. It would have been tremendously burdensome to do so at that point. You could do it, but it would be wholly ineffective. One of the differences today compared to 20 years ago is it was in the telephone company's interest to maintain telephone toll data because their billing was based on telephone toll data. Today that is no longer the case. In fact, the telephone companies see it as a burden, a storage burden, and, consequently, that information that was there in the telephone companies 20 years ago may well not be there today absent 215.

Senator LEE. Okay. Thank you very much, Director Mueller. I see my time has expired. Thank you. And thank you, Mr. Chairman.

Senator WHITEHOUSE. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

I join my colleagues in thanking you, Director Mueller, for your service, and I extend my aloha to you in your future endeavors.

I appreciate the fact that this kind of data that is collected, particularly under Section 215, could be helpful in connecting the dots. And, yes, it is hard to figure out which dot might be the critical

dot that helps you to foil a plot. So I have a question about, to the best of your knowledge, what are the costs of collecting and storing data gathered under Sections 215 and 702 of both your agency as well as NSA?

Mr. MUELLER. I would think you would have to turn to NSA to respond to that question. I am not familiar with what it costs.

Senator HIRONO. What about to your department, to the FBI?

Mr. MUELLER. We do not do the storage. NSA stores the 215 data.

Senator HIRONO. What about the collecting part?

Mr. MUELLER. The collecting?

Senator HIRONO. Yes, collecting of the data.

Mr. MUELLER. It goes directly to NSA. The order directs that the data go to NSA.

Senator HIRONO. So while you are the applicant for the collection of this data, it is NSA that I should ask about what the costs attendant to the data collection are.

Mr. MUELLER. Yes.

Senator HIRONO. Do you know how long the data collected under 215 is kept?

Mr. MUELLER. Five years.

Senator HIRONO. Just five years? Do you think it should be longer?

Mr. MUELLER. No.

Senator HIRONO. Okay.

Mr. MUELLER. I also do not think it should be shorter.

Senator HIRONO. Okay. Now, part of your department—FBI's purview is prosecutions in Indian country, and you talked about that briefly in your testimony. And the Department of Justice recently issued a report on investigations and prosecutions in Indian country during 2011 and 2012, and this is a report mandated by the Tribal Law and Order Act of 2010. And it seems that while there has been a noticeable increase in the number of violent crimes prosecuted, those new figures do not reflect that one-third of all reported Indian country crimes were closed administratively by the FBI before they ever reached the formal referral stage. Moreover, approximately 80 percent of those investigations that were administratively closed were violent crime related.

Can you shed some light on the reasons why so many FBI Indian country investigations are closed before referral to DOJ and specifically ways in which your department can better address and investigate violent crime in Indian country, which is still a very big problem?

Mr. MUELLER. Well, I think we all understand it is a very big problem, and I know the Department of Justice, in particular the Attorney General and the Deputy Attorney General, this is one of their substantial priorities, which is why you see an increase of prosecutions in Indian country.

I will have to get back to you on the figures relating to administrative closures. I am not certain if there has been an uptick in the number of administrative closures, why that is there. It may be consistent with the fact that we have done additional prosecutions. With additional prosecutions, there is additional scrutiny of the underlying case which has resulted in administrative closures. But I

would be just speculating. I would have to get back to you after looking at the issue.

Senator HIRONO. Yes, considering that this is a major issue in Indian country and to realize that in this report so many of these cases are closed, I am curious to know why. So could you provide that information to our Committee?

Mr. MUELLER. Yes.

Senator HIRONO. Senator Feinstein had a concern about the use of drones, and particularly with regard to the use of drones by the private sector. Do we have any special or specific legislation governing the use of drones by the private sector?

Mr. MUELLER. I am not aware of any.

Senator HIRONO. Do you think that we should be thinking about federal legislation to protect individuals' privacy with regard to the use of drones by the private sector?

Mr. MUELLER. I think there are a number of issues relating to drones that are going to have to be debated in the future as they become more omnipresent, not the least of which is the drones in airspace and the concerns you have on that, but also the threat on privacy. We already have to a certain extent a body of law that relates to aerial surveillance and privacy relating to helicopters and small aircraft and the like, which I think could well be adapted to the use of drones. But it is still in nascent stages, the debate, but it is worthy of debate and perhaps legislation down the road.

Senator HIRONO. Especially as the hearing that we had in one of our committees—I think it was this one—where these drones can be very, very tiny but store a lot of data and there could be cameras on it. I think this is a burgeoning concern for many of us.

With regard to the data that is collected under Section 215, in particular the millions and millions of pieces of information collected, NSA indicated that there were 300 queries that were made with regard to this data, and they have to forward those queries to you, and 10 to 12 cases were referred to you?

Mr. MUELLER. They will refer them to us when they have a U.S. number that comes out of their query.

Senator HIRONO. I think as a lay person, I am having some difficulty understanding what the process is, what NSA does with all this information, where you come in. There is some nexus between the NSA looking at this data, 300 queries, and then forwarding to you, say, 10 to 12 cases where they see some further investigation needs to occur. So what happens to all these other cases that—other numbers that were queried by NSA?

Mr. MUELLER. Well, when you are talking about 10 or 12 cases, these are cases where the identification of a number led to a terrorist case or corroborated other information we had in a terrorist case. But if you have NSA on a number in Yemen, for instance, and they want to know who from the United States is in contact with that number, you have got that number in Yemen, they take that number in Yemen and they run it against the database of numbers to see whether there is any number in the United States that is contacting that number in Yemen. And when that number comes out—we mentioned a couple of examples here—in, say, San Diego, they will refer it to us and say that there is a number in San Diego that is in contact with this number in Yemen which is terrorist re-

lated. We then go get a National Security Letter or other paper to determine who has that number, who is the subscriber to that number. And once we get the subscriber to that number, then we will build the investigation.

That is, in simplified form, what the process is about. But absent that capability, we would never identify that person in San Diego who is in contact with a terrorist group in Yemen, and that is what we did not pick up in 2001 where the intelligence community was on a number in Yemen and this individual, al-Mihdhar, ended up being in the United States, and had we had that program in place, we might well have picked up al-Mihdhar.

Senator HIRONO. So, in your view, in spite of the fact that there are literally billions of pieces of information collected and, in your view, the dot-connecting possibilities justify this kind of breadth of data collection?

Mr. MUELLER. Given all the precautions, given all of the constraints on the program, given the oversight of the program, yes. But it is the program as a whole, not just the fact of the accumulation of the records, but how it is handled and what kind of information comes from it.

I was asked earlier today, Why did we miss Boston? Why did we miss Fort Hood? There can be one piece of information that comes out of it that would prevent the attack. People will say that we were not sufficiently attentive to al-Awlaki email traffic; had we been, we would have stopped Fort Hood.

So to the extent that this provides dots for us to connect, it is very useful. You never know which dot is going to be the one that breaks the case. And to the extent that you remove the dots from the playing field, we just do not have those dots to connect.

Senator HIRONO. I certainly understand that.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Senator Flake.

Senator FLAKE. Thank you, and I want to echo the sentiments of my colleagues in thanking you for your long and dedicated service. I was fortunate to be on the Judiciary Committee in the House, and we had interactions there, and I have enjoyed the association we have had, and your candor always here, and I appreciate that.

I feel kind of like—well, I grew up with 10 brothers and sisters, and when the dessert plate is passed around and you are the last one and all the dessert is gone, and in this case all the questions have been asked and, to your credit, answered. I had some questions with regard to the information being held and how long, but you have pretty much answered those. But there was one thing that I still wanted to ask. This 215 has been around since 2001 in some fashion?

Mr. MUELLER. Probably 2001, 2002, but in this fashion since I think 2007.

Senator FLAKE. Okay. How has the legal interpretation, internal interpretation—you rely on your own memos that you produce to interpret 215 and what you are able to ask and what kind of standard is applied. Has that changed over time since 2007 or perhaps before?

Mr. MUELLER. Well, prior to 2007—I am not certain what year it happened, but it was placed within the *FISA* Court, I think, be-

ginning in 2007. And while, yes, the Justice Department has made application to the *FISA* Court, the *FISA* Court has interpreted 215 to allow this program. So it is not just the Justice Department opining on what it thinks 215 means. It is the *FISA* Court that has issued opinions saying this is the appropriate interpretation of 215.

Senator FLAKE. All right. One question on the holding of data. You hold it for five years, and if it has not been queried or minimized during that period, then you get rid of it.

Mr. MUELLER. Yes.

Senator FLAKE. But that—

Mr. MUELLER. NSA holds it.

Senator FLAKE. NSA, yes. But that which has been queried and then duly minimized where appropriate, I assume that can be queried again and again during that five-year period. You say last year it was queried 300 times. It is the same information basically that—or the same database, the same metadata that is queried again and again.

Mr. MUELLER. But the database is refreshed each day, so that which is five years old is dismissed from the database, and the database picks up new numbers.

Senator FLAKE. All right. So it is just a rolling five-year period.

Mr. MUELLER. Yes.

Senator FLAKE. Anything older than five years—

Mr. MUELLER. Yes, which enables us to go back—you may have a number called in—for instance, al-Mihdhar out of San Diego made the call to the Yemen telephone number back in, I think, earlier in 2000. And so you needed that number in that database from a year before in order to tie in that particular number to the terrorist number in Yemen. And so it gives us that database for a period of time, which has the relevant information in it.

If you go to one of the providers, they may keep it for six months, may keep the data for 12 months, 16 months or 18 months, something along those lines. And so you would not be able to get the same data from the telephone carriers because they have no data retention responsibilities as you would get when we have that five-year database.

Senator FLAKE. All right. Well, thank you. Just in conclusion, your service will end sometime in September?

Mr. MUELLER. Yes.

Senator FLAKE. What advice would you give to this body in terms of what changes are needed moving forward in how we handle situations like this? Obviously, this came as a shock to most of the country that this kind of data was being collected in terms of—and you have concerns, and I share them, about too much information being out there. But what is the proper balance for this body to inform or to keep the citizens aware enough that their rights and their civil liberties are protected, but that we are also giving the appropriate federal agencies the tools that they need to thwart attacks? Is there any advice that you would give that you have not given before?

Mr. MUELLER. No, I would—the only thing I would say is that there are levels of transparency in this particular case where it is not necessarily always the case, it was not only Department of Justice, not only the Inspectors General—and we have had Inspector

General reports on these particular programs—but the *FISA* Court and Congress and various committees in Congress. And to the extent that each of those entities is brought into the loop and knows and understands, is able to question to a certain extent assuring that these entities have coverage, the American public has to put some faith in these institutions. You are always going to have those areas of—classified areas where it does not make any difference whether it is the cyber arena or the military arena or the intelligence arena like this, that disclosing our secrets will make us that much more vulnerable. There is always going to be a level of frustration.

The only other thing I would say is that there are going to be additional terrorist attacks. One of the most debilitating things for those of us in this particular—in our positions is to try your darnedest to prevent it but there be an attack, and then you are immediately attacked for why didn't you do more. And we always believe, regardless of the attack, that it is incumbent upon us and others to go back and do a scrub and see what we could have done better. But the tone of how you do that and the way that you do it would be helpful to those of us who worry about this day and night.

Senator FLAKE. Thank you. And thank you for your service.

Senator WHITEHOUSE. Senator Durbin.

Senator DURBIN. Thank you very much, Mr. Chairman.

Director Mueller, thank you so much for your service. I have enjoyed working with you over the years. I recall in particular when you arrived at the FBI after 9/11 and I took note of the fact that the computer system at the premier investigative agency for law enforcement in the United States of America on 9/11 was as archaic as anything anyone could imagine. The computer system you inherited at the FBI had no access to the Internet, had no word search capability, and was unable to transmit materials and documents. The photographs of the suspected terrorists on 9/11 were sent to the FBI offices across America by overnight mail because they could not be sent by the computer system that you inherited.

We had many conversations, some attempts, some missteps. Tell me today, where are we 12 years later in terms of the computer system of your agency?

Mr. MUELLER. One of the reasons for staying the last couple years was to get over the hump in terms of the computer systems. We have this computer system called Sentinel that has been operative for the last two years. It is cutting edge in terms of case management. Many of our other programs we are not only upgrading but are not incorporating in a much more effective network. But I will tell you, one of the most frustrating aspects of this job is trying to adapt new technology in an institution that has unique business practices and to try to modify those business practices at the same time—and upgrade those business practices at the same time you are trying to adapt to new technology, particularly with the contracting mechanisms within the Federal Government where, if you have a five-year contract, things are going to change, new technologies are going to come along. And the fact of the matter is there is very little room in those contracts for any ability to change to adapt to the times.

But if you had seen—I vividly remember being in our intelligence—what we call SIOC—intelligence operations room on September 11th and the paper stacked up, and in Boston we were back in the same place, and there is not a piece of paper to be seen. And also to the credit of the Bureau, the ability to identify those two individuals in Boston within 48 hours after it occurred, utilizing the various technologies in our laboratory as well as up there is, I think, testimony to the fact—testament to the fact that we have come a long way. Still a ways to go, but we have come a long way.

Senator DURBIN. Well, let me just say for the record, in addition to bringing integrity to the position, which you have, in addition to helping keep America safe with an extraordinary degree of success, I think your legacy is going to include this, that the information technology available in your department is now meeting 21st century standards, where when you inherited it, it was, as you say, a creation of “unique business practices.” I think you are being very kind in that characterization.

Mr. MUELLER. Can I just add one thing? We are okay today, but as you well know, technology costs money. And with sequestration, I will put in another plug; this is an issue that all too often gets overlooked and perhaps cut, and it should not be because you cannot run an institution like ours unless you stay current with the latest technology.

Senator DURBIN. Sequestration, the way it has been characterized, the way it has been implemented, is a pervasive problem. I met yesterday with Director Clapper, and he talked about the impact of sequestration on doing checks on employees for security clearances. We have had to reduce the number of checks of those current employees when it comes to security. And now we are dealing with one former contractual employee who has disclosed things which were very important to our national security.

Speaking of that issue, on Section 215, which you have been queried about quite a bit, I have offered an amendment over the years to try to limit the metadata collection in terms of specific suspicion. That was the original standard. It eventually was changed with *FISA Act* reauthorization.

But yesterday the Department of Justice—I hope you are aware of—released publicly, according to reports we have, the standards for searching the database of phone records when there is “reasonable suspicion” based on specific and articulated facts that the information sought is “associated with a specific foreign terrorist organization.” The standard that they released yesterday, which they are now going to use, is actually stricter than the standard that I have been proposing over the years for the limitations on 215.

Can Section 215, do you believe, be revised to require connection to a suspected terrorist without affecting the ability to obtain useful information?

Mr. MUELLER. I am a little bit confused because what we call the “selector,” the telephone number that is run against the database, has to be identified as being—how do I say it?—meeting the reasonable suspicion standard with regard to terrorist attacks, that particular phone number, that is an appropriate standard for that particular phone number, because you cannot pick a phone number

out of the blue or for some other thing. You have to have it tied into terrorism, and then it is pushed against the database.

Now, I do not know whether your standard as you were supporting it is the standard you apply to collection of the records or the standard you apply to identifying the selector against the—what you are going to use—what you are going to put against the database. So if you—

Senator DURBIN. Our standard is on the collection of the records.

Mr. MUELLER. See, I think that is a little bit different. The standard we are talking about here is the identification of the selector that you are going to run against that database of records.

Senator DURBIN. So if the provider, if the telephone provider, for example, were to retain the records for five years and you would have access, through our government agencies and through our processes, to access those records for government purposes if there is a suspicion, would that meet the needs of collecting the information to keep us safe?

Mr. MUELLER. Not in the same way the program does now for several reasons. First of all, you would have to go to a number of telephone companies. You would have to get legal process and go to a number of telephone companies. Then you have to hope that those telephone companies have some records retention capability. I can assure you it is not going to be five years.

Senator DURBIN. Not today.

Mr. MUELLER. Not today.

Senator DURBIN. It could be required of them, though.

Mr. MUELLER. It could be. It could be. I am not saying it could not be done, but you are asking me if there is a distinction between the program run today and how you propose to perhaps amend it. And there are some downsides. You know, the balance is for Congress to decide, but there are downsides in terms of the time it would take to serve it, the time it would take for them to get it, and in every one of these cases, time is of the essence. You do not want to have to delay six months or a year to get the information to prevent the next terrorist attack.

Senator DURBIN. You have been very patient with your time, and I thank you for your service, Director Mueller.

Mr. MUELLER. Thank you.

Senator DURBIN. I wish you the best.

Mr. MUELLER. Thank you.

Senator WHITEHOUSE. So I am last, Director.

Mr. MUELLER. Happily so. Happily so.

Senator WHITEHOUSE. Good to see you. There are three topics I want to touch on.

The first has to do with the investigation into the conduct of the IRS. The background to this is that the tax laws allow you to form up as a charity under Section 501(c)(3), but if you want to lobby, you have got to form up under 501(c)(4). And then if you actually want to electioneer, you have got to form a so-called super PAC.

The difference between a 501(c)(4) and a super PAC, as you know, is that a super PAC is required to disclose its donors. So what developed was a pattern of folks filing as a 501(c)(4) but then going out and electioneering as if they were a super PAC. And the problem with doing that is that there is a place on the form, when

you file for a 501(c)(4), that requires you to assert and aver under oath that you will not seek to influence elections and so forth.

So there appears to me—we had a hearing on this in the Committee—to be almost a lay-up case for 18 U.S.C. 1001 false statement violations based on what appear on their surface—again, this requires investigation before you can make any final determination, but it appears on the surface that these are flagrantly false statements made under oath to a government agency for the purpose of misrepresenting the intentions of those forming the 501(c)(4).

That never comes to the FBI because there is an agreement between the Department of Justice and the IRS that unless the IRS has put a case together and forwarded it, we are not going to look at it. And I think the 501(c)(4) applicants were taking advantage of that, and the IRS was feeling a bit intimidated because there were some very powerful people in this country on both sides of the aisle behind the problem, behind the 501(c)(4) problem.

So I hope that as you are looking at the IRS question, part of what you are looking at is whether or not something that, as you and I both know, is really a plain vanilla prosecution, a false statement case, is something that the FBI should turn away from because the IRS has not yet referred it when it is kind of out in the plain light of day. And I hope that you will consider that question as the IRS investigation moves forward.

It may not be the kind of question that leads to a charge. It may not be purely investigative. But I think it is an important policy question, and I think it is important for the American people to know that when people are doing something that appears on its face—again, subject to rigorous investigation and proof, but appears on its face to be a flagrant false statement, the answer from the government, “Yes, but it was not referred to us in the right way,” is not a very convincing answer to what appears to be a fairly blatant criminal act—not a very major one, but a very blatant one.

So I would like to ask your comment on that, if that is something that you will consider as part of your look at this.

Mr. MUELLER. I am not familiar with any such agreement. I will have to look at that and discuss it and see what—

Senator WHITEHOUSE. Okay. We will make that a question for the record, and you can get back to me later.

Mr. MUELLER. Fine.

Senator WHITEHOUSE. Now, the second is we met recently with some of your folks, some of the Department of Justice folks, in the Office of Management and Budget to try to figure out how our prosecutorial and investigative law enforcement resources should be structured to focus on the cyber problem. And in the time that I have been in the Senate, six years now, I have watched that administrative structure morph really almost every year to something new, something different. And I have been out to NCIJTF and some of your facilities, and I applaud and am impressed by how hard the FBI works to keep track of who is coming in the doors and windows attacking our country and our companies and trying to get those alerts out as quickly as they can to the companies that are being attacked and having their intellectual property stolen.

But it has not resulted in a lot of prosecutions, and as best I know, there is not a single case that has ever been prosecuted of a pure industrial espionage, cybersecurity attack from outside the country on an American company.

There has always been something involved, a CD that got stuck in somebody's pocket, but the pure hack, I am not aware of a case that has been made yet, and that is a question I ask pretty frequently.

I think this is a boom area. I am delighted and pleased that the administration in a time when most other parts of the government are being asked to cut, is actually investing more in cybersecurity at the FBI, at the Department of Justice, at the NSA, at the Department of Defense, and at other places, because it is a huge vulnerability, I believe. And I know you are on your way out, but I hope that one of your departing messages to the Bureau will be we need to keep looking forward to see what our structure should be to take on this threat in the years ahead. I do not think we are there yet. I think we have made immense progress. I think we are in a state of constant flux as we try to adapt to the problem. But when you look at a problem that is described by very senior officials as us being on the losing end of the biggest transfer of wealth by illicit means in human history, basically because the Chinese are raiding our corporations and stealing our intellectual property in a nutshell, that is a pretty serious problem set. And it is only going to get worse because it has its transnational sabotage and its multinational criminal components as well. And I hope that you guys have an open mind and have somebody detailed to looking forward and saying, "What does this look like down the road? How should this be structured so we are really after it?"

When we had the drug problem, we started a DEA to handle it. What is the structure this should look like down the road? And I know it is such a mad scramble right now and you are working so hard and people are doing such a great job. It is hard to kind of pop your head up out of the day-to-day fight and plan ahead, but I think that would be a good legacy for you to leave, that that was a look forward and let us see what this thing should be like five, 10 years from now.

Mr. MUELLER. I would venture to say anybody in the Bureau knows the focus has been over the last year on cyber in a variety of ways, and we have to put our own house in order first.

Senator WHITEHOUSE. Yes.

Mr. MUELLER. And we are doing that. We are not there yet, but we have to adapt over the next several years, an organization that lends itself to addressing itself with more specificity to particularized threats that have been prioritized, of which cyber will be a substantial one. We now have entities, counterintelligence and cyber, because they are like that. And our organizational structure has morphed into a threat-based organizational structure as opposed to a program organizational structure. And we have got to continue to do that.

One of the focal points outside the FBI, though, is the NCIJTF, my firm belief that for us to be successful, we have to have people at the table right at the outset, and determine whether it is national security or criminal or what have you, but you need all of

the facts, all of the information on the table, regardless of the classification side, because there may be something up there that will help you on a criminal matter down below, but have everybody in—the relevant players in the government working at NCIJTF or some comparable facility.

And then last, with the private sector. Once we have our act together administratively and have—my own belief is generally collocation with the exception of NSA because of what they have got, but the rest of us to be relatively collocated, then in my mind you need the partnerships in the private sector to come together and equip themselves to share information and then set up conduits between the private sector and the Federal Government that will assure privacy but also enable us to share information in ways that we have not been able to or had to in the past.

So I think we are moving toward that structure, but we have a way to go, and I can tell you with my successor, we will have some discussions on this.

Senator WHITEHOUSE. Good. The last point, we have addressed it a little bit, but I would like to make the point that I do think that we overclassify. It is much easier to classify than it is to declassify. There are a whole variety of reasons—some good and some not so good—for classifying programs and classifying materials. But it seems to me that a lot of the stuff that has been said about the NSA programs and about the FBI's support of them could easily have been said beforehand without compromising those programs in any significant respect, particularly the multiple checks and balances, the number of guards at the door to the vault before anybody can get any kind of information, both Houses of Congress being briefed in on programs like this, Inspectors General being independently accountable to review programs like these, the internal oversight of the executive branch, apart from the independent Inspectors General, and the rigor and frequency of the audit that is done for those programs, the fact that regular line United States district court judges are brought in on detail to serve on the *FISA* Court, and they have to in various ways sign off on these programs. You have as strong an array of protections under our system of separated government as one could possibly create, I believe. I do not know that a single stone has been left unturned in terms of putting eyeballs onto making sure that these programs were carefully used and never abused.

So that kind of story, I think, is one that does not hurt us to get out first. Before this incident, people knew that there were ways in which we were protecting ourselves, and we could have said generally that, without getting into the details of any of these programs, when we look into programs that affect Americans' privacy, we go all in on making sure that there are not short cuts, making sure that only qualified people get it.

And so I think the lesson from this going forward is that as much as there is a public interest in classification of a lot of this information, there is also a public interest in declassifying it. And in some cases, I would contend that declassification has exactly zero national security risks associated with it. It just kind of got swept up with a bunch of other stuff because the program is classified. And we depend on you to do this because Senators are not declassifiers.

The only way that the Senate Intelligence Committee can declassify anything is so complicated that it has never been used in the history of the Senate Intelligence Committee.

So I would urge you to—I am speaking through you now, I think, to a whole lot of other people as well. But I do think that a more persistent focus on what could be declassified and what would help for these foreseeable events of disclosure would be a good policy to pursue.

Your thoughts?

Mr. MUELLER. I understand your sentiments. I do believe there is a price to be paid. We tend to think that people know and understand the Internet around the world. But you have persons who want to undertake terrorist attacks that do not have a full understanding of the Internet. And to the extent that you expose programs like this, we are educating them. We are educating them about how the Internet works actually worldwide. We are educating them as to what our capabilities are, and the brighter and the smarter of them will be educated and find other ways to communicate, and we will not pick up communications we want.

Now, that is not to say that the scale should not be on the other side. It is much easier to explain to the public when you do not have the restrictions, quite obviously, of classification. All I am saying is I do think there is a price to be paid. Not always. There are occasions where we can declassify things. But I would not underestimate the price to be paid by a substantial—let me just put it, substantial disclosures.

Senator WHITEHOUSE. Yes, I agree. I think we have to be very sensitive to that, and we have to be particularly sensitive to that when we are talking about the operating mechanics of a particular program. But when we are telling the American people—we are not going to raise the question of what we are doing, but we want you to know that when, as, and if we do anything, here are the kind of procedures we use. You would never tell anybody about an ongoing investigation. But we tell everybody about the warrant requirement, about minimization, about the things that protect Americans' security. And that process is also classified when it comes to these NSA programs.

Mr. MUELLER. Good point. I got you.

Senator WHITEHOUSE. That is where I think we can make some ground.

This is, I think, the end of your last appearance before this Committee, so let me thank you very much. You have been a terrific Director of the Federal Bureau of Investigation. Before that you were a terrific member of the Department of Justice and a terrific United States Attorney. You have made an awful lot of people proud, sir, and we are very glad to have had the chance to work with you.

Mr. MUELLER. Well, thank you for that, but it is the men and women of the FBI that make the place run, as you and I both know, having been in comparable positions. But thank you.

Senator WHITEHOUSE. Well said. Thank you.

For the record, the record will remain open for a period of one week if anyone wants to add to the record.

[Whereupon, at 12:22 p.m., the Committee was adjourned.]

A P P E N D I X

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List

Hearing before the
Senate Committee on the Judiciary

On

“Oversight of the Federal Bureau of Investigation”

Wednesday, June 19, 2013
Dirksen Senate Office Building, Room 106
10:00 a.m.

The Honorable Robert S. Mueller, III
Director
Federal Bureau of Investigation
United States Department of Justice
Washington, DC

PREPARED STATEMENT OF CHAIRMAN PATRICK LEAHY

**Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee
Hearing On Oversight Of The Federal Bureau Of Investigation
June 19, 2013**

Today, the Judiciary Committee welcomes Robert Mueller for what is likely to be his final appearance before this panel as Director of the Federal Bureau of Investigation (FBI).

Director Mueller began as head of the FBI just days before the terrorist attacks of September 11, 2001. For nearly 12 years, he has led the Bureau as it has shifted its primary focus to national security and counterterrorism efforts, while still carrying on its historic mission of fighting crime. That transition, while important for our national security, has not been without problems. From National Security Letters to the latest revelations about the use of the PATRIOT Act, I remain concerned that we have not yet struck the right balance between the intelligence-gathering needs of the FBI, and the civil liberties and privacy rights of Americans. I also want to make sure that the shift in the FBI's focus does not unduly hamper the Bureau's ability to investigate cases involving fraud and violent crime that significantly affect the everyday lives of Americans.

Notwithstanding these concerns, I have never questioned the integrity, dedication, and consummate professionalism of Director Mueller, as he has led the Bureau through very difficult times. He has been a steady and determined leader of the FBI. He has spoken forcefully about the need to protect Americans' civil liberties, as he did at the 100th anniversary of the Bureau. It was no surprise that a committed public servant like Bob Mueller would agree to put his long-awaited vacation and travel plans on hold, so that he could continue to serve his country in this intensely demanding position, when the President asked him to stay on board two years ago. Director Mueller has devoted his entire life to public service, and we are grateful to him and his family for their continued sacrifice. Bob Mueller will be leaving the next FBI Director enormous shoes to fill.

As the FBI now prepares for its first change in leadership since the 9/11 attacks, we must continue to review closely the broad intelligence-gathering powers that Congress granted to the FBI in order to combat terrorist threats. The FBI has faced daunting national security challenges, but we must also ensure that they do not violate the privacy rights and civil liberties of law-abiding Americans. I have long said that protecting national security and protecting Americans' fundamental rights are not mutually exclusive. We can and must do both.

The recent public revelations about two classified data collection programs illustrate the need for close scrutiny by Congress of the Government's surveillance activities. For years, I have been troubled by the expansive nature of the USA PATRIOT Act. These powerful law enforcement tools, including Section 215 orders, require careful monitoring and close oversight. That is why I authored legislation in 2009 that would have improved and reformed the PATRIOT Act, while increasing public accountability and transparency. My bill was reported by this Committee on a bipartisan basis in 2009 and 2011, and would help protect the privacy rights of innocent Americans, and strengthen oversight by the courts and Congress. I intend to re-introduce that bill tomorrow, and hope that Senators from both parties will join me in this effort to improve the

PATRIOT Act and further protect the civil liberties of everyday citizens. The American people deserve to know how broad investigative laws like the PATRIOT Act are being interpreted and used to conduct electronic surveillance, particularly when it involves the collection of data on innocent Americans. The American people also deserve to know whether these programs have proven sufficiently effective to justify their breadth. Right now, I remain skeptical.

I also firmly believe that we need to maintain close oversight over the broad surveillance authorities contained in the FISA Amendments Act. Since enactment of this law in 2008, I have had concerns about the scope of Section 702, despite its statutory focus on foreigners overseas. That is why I pushed for a shorter sunset, greater transparency and better oversight last year when Congress considered reauthorizing these provisions. Regrettably, the Senate rejected my efforts. I will continue to push for those commonsense improvements, as well.

It is important that Congress is able to conduct an open debate about the efficacy of these tools, particularly in light of the Boston Marathon bombing in April. We must carefully examine not only the tools that allow the Government to collect information, but also what we do with that information. I remain concerned that intelligence obtained by the FBI may not have been properly relayed through the Joint Terrorism Task Force to the Boston Police Department or to other law enforcement authorities both here and abroad. That is why I am glad that the Inspector General for the Intelligence Community is conducting an independent assessment of the intelligence gathering and sharing that led up to the Boston bombings.

Finally, the FBI's increased focus on counterterrorism over the past decade must not come at the expense of the Bureau's essential law enforcement functions. Despite the recent economic crisis and times of shrinking state and local law enforcement budgets, we have been fortunate to see crime rates across the country decline. However, preliminary data released earlier this month shows that in 2012, the overall violent crime rate in the United States rose for the first time since 2006. We must examine the reasons for this uptick in violent crime, and how the FBI intends to continue working with its state and local partners to ensure that this trend does not continue. I also know that the FBI has been at the forefront in using forensic science in its investigations, and while it has had its fair share of problems in the past with its own crime lab, I look forward to working with the FBI as I develop comprehensive legislation to address forensic science reform.

I thank Director Mueller for appearing before the Committee, for his responsiveness to our oversight efforts, and for his personal example and impressive leadership over the past 12 years in returning the FBI to its best traditions. Most importantly, I thank the hardworking men and women of the FBI, with whom I know he is proud to serve, and I look forward to the Director's testimony.

#

PREPARED STATEMENT OF HON. ROBERT S. MUELLER III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC



Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

JUNE 19, 2013

Statement for the Record
Robert S. Mueller, III
Director
Federal Bureau of Investigation

Committee on the Judiciary
U.S. Senate

“Oversight of the Federal Bureau of Investigation”
June 19, 2013

Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

Today's FBI is a threat-driven, intelligence-led organization. We have built a workforce and leadership team that view continuing transformation as the means to keep the FBI focused on key threats to our nation.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our national security, our economy, and to our communities.

Counterterrorism remains our top priority. As illustrated by the recent attacks in Boston, the terrorist threat against the United States remains very real.

Yet national security is not our sole focus – we remain committed to our criminal programs. In the economic arena, investment fraud, mortgage fraud, and health care fraud have undermined the world's financial systems and victimized investors, homeowners, and taxpayers.

At the same time, gang violence, violent crime, crimes against children, and transnational organized crime pose real threats in communities across the country.

These diverse threats facing our nation and our neighborhoods underscore the complexity and breadth of the FBI's mission. To do this, we in the Bureau are relying on our law enforcement and private sector partners more than ever before.

Yet regardless of the challenges we face, the FBI remains firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the citizens we serve.

I look forward to working with this committee in these final months of my term to ensure that the FBI maintains the capabilities needed to address these diverse threats now and into the future.

Counterterrorism

Over the past two months, we have seen an extraordinary effort by law enforcement, intelligence, and public safety agencies to find and hold accountable those responsible for the Boston bombings.

I would like to thank those who have worked tirelessly in the pursuit of safety and justice. These collaborative efforts, along with the public's help, enabled us to identify the individuals who we believe are responsible for this attack. Our thoughts and prayers remain with the bombing victims – those who perished and those who are embarking on a long road to recovery.

As this case illustrates, we face a continuing threat from homegrown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often distinct, but they are increasingly savvy and willing to act alone, which makes them difficult to identify and to stop.

In the past two years, we have seen homegrown extremists attempt to detonate IEDs or bombs at such high profile targets as the Federal Reserve Bank in New York, commercial establishments in downtown Chicago, the Pentagon, and the U.S. Capitol. Fortunately, these attempts, as well as many others, were thwarted. Yet the threat remains.

Overseas, the terrorist threat is similarly complex and ever-changing. We are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Al Qaeda and its affiliates, especially al Qaeda in the Arabian Peninsula (AQAP), continue to represent a top terrorist threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

In December 2011, Somali national Ahmed Abdulkadir Warsame pled guilty to nine counts of providing material support to AQAP and al Shabaab. A Joint Terrorism Task Force investigation found that Warsame conspired to teach terrorists how to make bombs, provided explosives weapons and training to al Shabaab and arranged for al Shabaab leaders to obtain weapons from members of AQAP. Warsame faces up to life in prison.

Counterintelligence

We still confront traditional espionage – spies posing as diplomats or ordinary citizens.

But espionage also has evolved. Spies today are often students, researchers, or businesspeople operating “front companies.” And they seek not only state secrets, but trade secrets, research and development, intellectual property, and insider information from the federal government, U.S. corporations, and American universities.

They continue to grow more creative and more sophisticated in their methods to steal innovative technology, eroding America's leading edge in business and posing threats to national security. In the past four years, the number of arrests related to economic espionage has doubled, indictments have increased four-fold, and convictions have risen six-fold.

The loss of critical research and development data, intellectual property, and insider information poses a significant threat to national security.

In March, Steve Liu, a Chinese national and former employee of a New Jersey defense contractor, was sentenced to more than five years in prison for stealing thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, and drones. Liu traveled to China and delivered presentations about the technology at several Chinese universities.

These cases illustrate the growing scope of the "insider threat" — when trusted employees and contractors use their legitimate access to information to steal secrets for the benefit of another company or country. This threat has been exacerbated in recent years as businesses become more global and increasingly exposed to foreign intelligence organizations.

We in the FBI are working to combat this threat. The Counterintelligence Division educates academic and business partners about how to protect themselves against economic espionage. We also work with the defense industry, academic institutions, and the general public to address the increased targeting of unclassified trade secrets across all American industries and sectors.

And we are focused on the possible proliferation of weapons of mass destruction. In July 2011, the FBI established the Counterproliferation Center to identify and disrupt proliferation activities. The center combines the operational activities of the Counterintelligence Division, the subject matter expertise of the WMD Directorate, and the analytical capabilities of the Directorate of Intelligence. Since its inception in July 2011, the Counterproliferation Center (CPC) has overseen the arrest of approximately 50 individuals, including several considered by the U.S. Intelligence Community to be major proliferators.

For example, Lu Futain pled guilty on November 18, 2011, to federal charges of selling sensitive microwave amplifiers to the People's Republic of China (PRC). Lu was sentenced to 15 months in prison and three years of supervised release on October 29, 2012. Lu founded Fushine Technology, a corporation based in Cupertino, California, which exported electronic components used in communications and radar equipment. In April 2004, Lu's firm exported a microwave amplifier to co-defendant Everjet Science and Technology Corporation, a PRC-based company also owned by Lu, without having obtained a license from the U.S. Department of Commerce.

Susan Yip, a Taiwanese citizen, was sentenced to two years in prison on October 24, 2012, for helping obtain sensitive military parts for Iran in violation of the Iranian trade embargo. In her guilty plea, Yip admitted to using her Taiwan and Hong Kong-based companies to carry out a fraudulent scheme to violate the Iranian Transaction Regulations, by acting as a

broker and conduit for the purchase of items in the United States for shipment to Iran. From October 2007 to June 2011, Yip and her fellow conspirators obtained, or attempted to obtain, more than 105,000 parts valued at approximately \$2.6 million. Yip helped buy the parts without notifying U.S. suppliers that the parts were being shipped to Iran, and without obtaining the required U.S. Government licenses.

Together with our law enforcement and intelligence partners, we must continue to protect our trade secrets and our state secrets, and prevent the loss of sensitive American technology.

Cyber

The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas, threatening innovation. And as citizens, we are also increasingly vulnerable to losing our personal information.

That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

We in the FBI have built up a substantial expertise to address cyber threats, both here at home and abroad.

We have cyber squads in each of our 56 field offices, with more than 1,000 specially trained agents, analysts, and forensic specialists. We have hired additional computer scientists. The FBI also has 63 Legal Attaché offices that cover the globe. Together with our international counterparts, we are sharing information and coordinating investigations. We have Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players in the cyber crime arena.

Here at home, the National Cyber Investigative Joint Task Force comprises 19 law enforcement, military, and intelligence agencies to coordinate cyber threat investigations. We in the FBI work closely with our partners in the NSA and DHS. We have different responsibilities, with different "lanes in the road," but we must all be on the same page in addressing cyber threats.

The leaders of the FBI, DHS, and NSA recently met to clarify the lanes in the road in cyber jurisdiction. Together, we agreed that the DOJ is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. DoD's role is to defend the nation, gather intelligence on foreign cyber threats, and to protect national security systems.

Although our agencies have different roles, we also understand that we must work together on every substantial intrusion, and to share information among the three of us. Notification of an intrusion to one agency will be notification to us all.

In addition, the private sector is a key player in cyber security.

Private sector companies are the primary victims of cyber intrusions. And they also possess the information, the expertise, and the knowledge to be an integral partner in reducing instances of cyber crime.

In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance – a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the Alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and manufacturing. The members of the Alliance work together with federal and international partners to provide real-time threat intelligence, every day.

Another initiative, the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems – together.

We intend to further strengthen the bridges we have built between the federal government and the private sector in the cyber security realm. We must fuse private-sector information with information from the Intelligence Community and develop channels for sharing information and intelligence quickly and effectively.

Our success in resolving cyber investigations rests on the creative use of investigative techniques we have used throughout the FBI's history – physical surveillance, forensics, cooperating witnesses, sources, and court-ordered wire intercepts.

One example concerns the hacker known as "Sabu" – one of the co-founders of the hacktivist group LulzSec.

The case began when our Los Angeles Division collected numerous IP addresses used to hack into the database of a TV game show. Our New York Office used a combination of investigative techniques, including human sources, search warrants, and surveillance, to identify and locate Sabu.

We went to arrest him, and we gave him a choice: go to jail now, or cooperate.

Sabu agreed to cooperate, and he became a source, continuing to use his online identity. His cooperation helped us to build cases that led to the arrest of six other hackers linked to

groups such as Anonymous and LulzSec. It also allowed us to identify hundreds of security vulnerabilities – which helped us to stop future attacks, and limit harm from prior intrusions.

Defeating today's complex cyber threats requires us to continually evolve and adapt.

Instead of just building better defenses, we must also build better relationships. And we must overcome the obstacles that prevent us from sharing information and, most importantly, collaborating.

U.S. law enforcement and the Intelligence Community, along with our international and private sector partners, are making progress. However, technological advancements and expansion of the Internet continue to provide malicious cyber actors the opportunity to harm U.S. national security and the economy. Given the consequences of such attacks, the FBI must keep pace with this rapidly developing and diverse threat.

Criminal

With regard to criminal threats, our responsibilities range from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises, and from violent crime to public corruption. These criminal threats pose a significant threat to the safety and security of our communities.

Public Corruption

Public corruption is the FBI's top criminal priority. We have had a number of successful investigations in this area in recent years, including a racketeering indictment handed down in April. Twenty-five individuals, including 13 Maryland correctional officers, allegedly conspired with the Black Guerrilla Family gang inside prisons to distribute drugs and launder money. Gang members allegedly bribed correctional officers at several Maryland prison facilities, convincing them to smuggle in drugs, cell phones, and other contraband. The correctional officers alerted imprisoned gang members of upcoming cell searches and several of the officers had long-term sexual relationships with the gang members and were impregnated by them. The defendants face maximum sentences of 20 years in prison.

Financial Crimes

We have witnessed an increase in financial fraud in recent years, including mortgage fraud, health care fraud, and securities fraud.

Mortgage Fraud

The FBI and its partners continue to pinpoint the most egregious offenders of mortgage fraud. As of May, the FBI had nearly 2,000 mortgage fraud investigations nationwide — and nearly three-fourths of these cases included losses of \$1 million or more.

With the economy and housing market still recovering in many areas, we have seen an increase in schemes aimed at distressed homeowners, such as loan modification scams and phony foreclosure rescues.

Others seek to defraud lenders by submitting fraudulent loan documents and setting up straw buyers to purchase homes. The homes then go into foreclosure, the banks are left holding the bag, and neighborhoods are left to manage the blight associated with vacant properties.

Last month, the leader of a \$66 million mortgage fraud scheme was sentenced to eight years in prison after arranging home sales between straw buyers and distressed homeowners. Gerard Canino, 51, from Long Island, New York, along with his co-conspirators, obtained mortgage loans for sham deals by submitting fraudulent applications to banks and lenders. The lenders sent the mortgage proceeds to the conspirators' attorneys and the attorneys submitted false statements to the lenders about how they were distributing the loan proceeds. They then distributed the loan proceeds among themselves and other members of their conspiracy.

Over the past five years, we have continued to boost the number of Special Agents investigating mortgage fraud. Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud.

We also work closely with the Department of Housing and Urban Development, Postal Inspectors, the IRS, the FDIC, and the Secret Service, as well as with state and local law enforcement offices.

Health Care Fraud

Health care spending currently makes up about 18 percent of our nation's total economy — and that percentage will continue to rise as our population ages. The federal government projects that by 2021, health care spending will reach 20 percent of the U.S. economy. These large sums present an attractive target for criminals — so much so that we lose tens of billions of dollars each year to health care fraud.

Last month, the Medicare Fraud Strike Force — a partnership between the Department of Justice and the Department of Health and Human Services — arrested 89 individuals, including doctors, nurses, and other licensed medical professionals, for allegedly participating in Medicare fraud schemes costing more than \$223 million in false billing.

Since its inception in March 2007, Medicare Fraud Strike Force operations have charged more than 1,500 individuals who collectively have falsely billed the Medicare program for more than \$5 billion.

Health care fraud is not a victimless crime. Every person who pays for health care benefits, every business that pays higher insurance costs to cover their employees, every taxpayer who funds Medicare, is a victim. Schemes can cause actual patient harm, including

subjecting patients to unnecessary treatment, providing sub-standard services and supplies, and passing potentially life-threatening diseases due to the lack of proper precautions.

As health care spending continues to rise, the FBI will use every tool we have to ensure our health care dollars are used to care for the sick — not to line the pockets of criminals.

Corporate and Securities Fraud

Another area where our investigations have increased substantially in recent years is in corporate and securities fraud. From September 2008 to April 2013, the FBI has seen a 36 percent increase in these cases, to more than 2,750 today.

One of our largest securities fraud cases centered on the Stanford Financial Group – a Houston, Texas, financial company that caused \$7 billion in losses and impacted more than 30,000 victims. Using evidence obtained throughout the investigation, the FBI identified key executive management personnel who conspired to commit large-scale securities fraud. In January and February of 2013, the last of these co-conspirators were sentenced to prison. To date, five individuals have been sentenced, ranging from 3 years to 110 years in prison.

As financial crimes become more sophisticated, so must the FBI. In the post-financial crisis period, the FBI devoted an additional 150 Special Agents and more than 175 forensic accountants to combat evolving financial crimes.

In addition to the dedication of more personnel, the FBI continues to use sophisticated techniques, such as undercover operations and Title III intercepts, to address these criminal threats. These techniques have been widely known for their successful use against organized crime, and they remain a vital tool to gain concrete evidence against individuals conducting crimes of this nature on a national level.

Finally, the FBI recognizes the need for increased cooperation with our regulatory counterparts. Currently, we have embedded agents and analysts at the Securities and Exchange Commission and the Commodity Futures Trading Commission, which allows the FBI to work hand-in-hand with U.S. regulators to mitigate the corporate and securities fraud threat. Furthermore, these relationships enable the FBI to identify fraud trends more quickly, and to work with our operational and intelligence counterparts in the field to begin criminal investigations when deemed appropriate.

Gangs/Violent Crime

For many cities and towns across the nation, violent crime – including gang activity – continues to pose a real and growing problem.

Gangs continue to become more sophisticated. They commit criminal activity, recruit new members in urban, suburban, and rural regions across the United States, and develop criminal associations that expand their influence over criminal enterprises, particularly street-level drug sales.

Gangs also have expanded their operations to alien smuggling, identity theft, and mortgage fraud. Our Violent Crime, Violent Gang/Safe Streets, and Safe Trails Task Forces target major groups operating as criminal enterprises – high-level groups engaged in patterns of racketeering. This allows us to identify senior leadership and to develop enterprise-based prosecutions.

Active Shooter Threats

Communities across America also continue to face active shooter and mass casualty incidents. Since the Sandy Hook tragedy last December, the FBI has been working with the Department of Justice's Bureau of Justice Assistance to provide tactical training to law enforcement agencies upon request.

One hundred FBI agents across the country have attended Advanced Law Enforcement Rapid Response Training (ALERRT) school and are prepared to train other officers in life-saving tactics. The 16-hour Basic Active-Shooter course prepares first responders to isolate any given threat, distract the threat actors, and end the threat. In addition, during the month of April, the FBI conducted two-day conferences and table top exercises with state, local, tribal, and campus law enforcement executives. We have also worked with experts at Texas State University to improve tactical training for officers that respond to active shooter situations and then held two-day conferences on active shooter situations at most of our 56 field offices nationwide. These conferences reached senior command staff from state, local, tribal and campus police agencies. These experiences gave behavioral experts, victim assistance specialists, and other personnel the opportunity to work through best practices and spurred discussions on how to best react to active shooter and mass casualty incidents. We are continuing our efforts with a new table top exercise specifically designed for campus law enforcement. This is an issue that impacts all of us, and the FBI is committed to working with our partners to protect our communities.

Transnational Organized Crime

We continue to confront organized crime. Crime syndicates run multi-national, multi-billion-dollar schemes – from human trafficking to health care fraud, and from computer intrusions to intellectual property theft.

These sophisticated enterprises come from every corner of the globe. Often they operate both overseas and in the United States, and include Italian, Russian, Asian, Balkan, Middle Eastern, and African syndicates as well as Outlaw Motorcycle Gangs. We work to cripple these national and transnational syndicates with every capability and tool we have: undercover operations; confidential sources; surveillance; intelligence analysis and sharing; forensic accounting; multi-agency investigations; and the power of racketeering statutes that help us take down entire enterprises. We also work closely with our international partners – in some cases, swapping personnel – to build cases and disrupt groups with global ties.

In the spring of 2012, four members of an Armenian organized crime ring were convicted in one of the largest bank fraud and identity theft schemes in California history. Two of those

convicted directed the scheme from behind bars. Using cell phones that were smuggled into a California state prison, they coordinated with others to obtain confidential bank profile information and stole money from high-value bank accounts. The six-year conspiracy cost more than \$10 million in losses to victims throughout the Southwest.

Crimes Against Children

The FBI remains vigilant in its efforts to keep children safe and to find and stop child predators. Our mission is threefold – first to decrease the vulnerability of children to sexual exploitation through awareness; second, to provide a rapid and effective federal investigative response to crimes against children; and, third, to enhance and assist the capabilities of state and local law enforcement investigators through task force operations.

Through our entire Violent Crimes Against Children program, including the Child Abduction Rapid Deployment Teams, the Innocence Lost National Initiative, the Office of Victim Assistance, Innocent Images program, and numerous community outreach programs, the FBI and its partners are working to make the world a safer place for our children.

And as new technology and new tactics are used to lure our young people, we must evolve in our efforts to stop those who would do them harm.

In January, a 31-year-old man from Montgomery, Alabama, was sentenced to 35 years in prison for producing child pornography through a massive online sextortion scheme. Christopher Patrick Gunn reached out to hundreds of young girls, gained their trust and their personal information, and then threatened to reveal that information unless they sent sexually explicit images of themselves. Gunn victimized children in at least a half-dozen states and Ireland.

This case came to light after junior high school aged-victims contacted their local police in a small Alabama town. Authorities soon realized there were strikingly similar cases in Mississippi and Louisiana.

By combining our resources and using our partnerships with state, local, and international law enforcement, we are able to investigate crimes that cross geographical and jurisdictional boundaries.

In April, we apprehended Eric Justin Toth, who had been added to the FBI's Ten Most Wanted Fugitive list in April 2012, and is currently charged with production and possession of child pornography. Toth, who also used the name David Bussone, is a former camp counselor and private-school teacher who taught here in Washington, D.C. He had been on the run since 2008, after an FBI investigation revealed pornographic images on a camera in his possession while at the school where he taught. A recent tip led law enforcement to Nicaragua, where Toth was living under an alias. He was apprehended in Esteli, Nicaragua, and has been returned to the United States to face prosecution.

And in February, the FBI's Hostage Rescue Team, crisis negotiators, and behavioral analysts were instrumental in rescuing a five-year-old boy in Midland City, Alabama. Working with the Dale County Sheriff's Department and the Alabama Department of Public Safety, some 300 officers and agents worked side-by-side to end a six-day siege in which an anti-government gunman named Jimmy Lee Dykes killed Charles Poland, a heroic school bus driver who died protecting the children on his bus. Dykes kidnapped the boy and held him hostage in an underground bunker. For six days, local, state, and federal negotiators spoke with Dykes and attempted to resolve the situation peacefully. When it was clear Dykes was becoming more and more agitated, authorities feared that the boy was in imminent danger. At that point, members of the Hostage Rescue Team entered the bunker in an attempt to rescue the boy. Dykes immediately attempted to detonate one of several bombs he had planted around his property and fired several shots at law enforcement. Dykes died during the confrontation. The boy was rescued safely, and incredibly, no law enforcement officials were injured.

This case represents some of the finest collaboration between local, state, and federal law enforcement agencies in recent time.

Indian Country

The FBI continues to maintain primary federal law enforcement authority to investigate felony crimes on more than 200 Indian reservations nationwide. More than 100 Special Agents from 20 different field offices investigate these cases.

Sexual assault and child sexual assault are two of the FBI's investigative priorities in Indian Country. Statistics indicate that American Indians and Alaska natives suffer violent crime at greater rates than other Americans. Approximately 75 percent of all FBI Indian Country investigations concern homicide, crimes against children, or felony assaults.

The FBI continues to work with tribes through the Tribal Law and Order Act of 2010 to help tribal governments better address the unique public safety challenges and disproportionately high rates of violence and victimization in many tribal communities. The Act encourages the hiring of additional law enforcement officers for Native American lands, enhances tribal authority to prosecute and punish criminals, and provides the Bureau of Indian Affairs and tribal police officers with greater access to law enforcement databases.

Currently, the FBI has 14 Safe Trails Task Forces that investigate violent crime, drug offenses, and gangs in Indian Country. In addition, the FBI continues to address the emerging threat from fraud and other white-collar crimes committed against tribal gaming facilities.

Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which

enables us to process fingerprint transactions much faster and with more accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's next-generation information and case management system was deployed to all employees on July 1, 2012. The system's indexing ability allows users to extract names, dates, vehicles, addresses, and other details, and to more efficiently share data with our law enforcement partners. Sentinel also enhances the FBI's ability to link cases with similar information through expanded search capabilities and to share new case information and intelligence more quickly among Special Agents and analysts.

The FBI shares information electronically with partners throughout the Intelligence Community, across the federal government, as well as with state and local agencies. For example, the FBI works closely with the nationwide Suspicious Activity Reporting (SAR) Initiative to ensure that SARs entered into the Justice Department's Information Sharing Environment's Shared Space system are simultaneously shared with eGuardian, the FBI's system used to collect and share terrorism-related activities among law enforcement, and in turn, delivered to the appropriate policing and Intelligence Community partners.

Going Dark

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge for conducting court-approved electronic surveillance of criminals and terrorists.

Court-approved surveillance is a vital tool for Federal, State, and local law enforcement authorities. It is, for example, critical in cyber cases where we are trying to identify those individuals responsible for attacks on networks, denial of service attacks, and attempts to compromise protected information. However, there is a growing gap between law enforcement's legal authority to conduct electronic surveillance, and its ability to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information to which it is lawfully authorized and that it needs to protect public safety, bring criminals to justice, and keep America safe. We must ensure law enforcement capabilities keep pace with new threats and new technology, while at the same time protecting individual privacy rights and civil rights.

It is only by working together – within the law enforcement and intelligence communities, with our private sector partners and with members of Congress – that we will find a long-term solution to this growing problem. In March, the FBI took one step toward improved collaboration and communication with the opening of the National Domestic Communications Assistance Center. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

Civil Rights / Civil Liberties / Rule of Law

Technology is one tool we use to stay a step ahead of criminals and terrorists. Yet as we in the FBI continue to evolve to keep pace with today's complex threat environment, our values must never change. The rule of law remains our guiding principle.

Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. For the men and women of the FBI, this is our guiding principle. In my remarks to New Agents upon their graduation from the FBI Academy, I emphasize that it is not enough to catch the criminal; we must do so while upholding his civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights make all of us safer and stronger. In the end, we will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

Conclusion

Chairman Leahy and Ranking Member Grassley, I thank you for this opportunity to discuss the FBI's priorities. The transformation the FBI has achieved during my term would not have been possible without your support and the support of the American people. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices throughout the United States and abroad, and we thank you for that support.

I look forward to any questions that you may have.

QUESTIONS SUBMITTED BY SENATOR SHELDON WHITEHOUSE FOR HON. ROBERT S.
MUELLER III

**Questions for the Record to Director Mueller Submitted by Senator Whitehouse
"Oversight of the FBI" – June 19, 2013**

A. FBI Computer Systems and Federal Contracting

In response to a question from Senator Durbin, you described the upgrades made to FBI computer systems during your tenure. You also noted that the federal contracting process, in which five-year contracts are common, made it a challenge to adapt to rapidly emerging and changing technologies.

In light of those comments please specify the contracting provisions that make it a challenge to adapt rapidly to emerging and changing technologies.

B. Campaign Finance

At a hearing of the Subcommittee on Crime and Terrorism on April 9, 2013 on "Current Issues in Campaign Finance Law Enforcement," the Subcommittee examined a pattern of what appear to be material false statements made to the government by 501(c)(4) organizations and organizations seeking 501(c)(4) status. These apparent false statements, which pertain to how much political activity the organizations have engaged in or plan to engage in, were made on IRS forms 1024 (application for exempt status), and 990 (return of exempt organization).

On first impression, these false statements would seem to violate both 18 U.S.C. § 1001 (false statements) and 2 U.S.C. § 7206 (fraud and false statements made under penalty of perjury).

Both the Department of Justice and the IRS have suggested that the Justice Department, and presumably the FBI, would not take an active role in investigating these apparent false statements until specific cases were referred by IRS to the Justice Department. This is in spite of the fact that 18 U.S.C. § 1001 false statement cases are, as Acting Assistant Attorney General for the Criminal Division Mythili Raman described them, "bread-and-butter" cases that investigators and prosecutors handle on a regular basis. Meanwhile, as a number of witnesses and experts have stated, the IRS is ill-equipped to investigate these cases. Neither the Justice Department nor the IRS was able to provide examples of any referrals having been made.

- Is it the case that the FBI does not investigate apparent criminal false statements on IRS forms absent a referral from the IRS, even where the apparent misconduct is already in the public record (such as through news accounts)? If so, what is the basis for this policy?
- Are you aware of any referrals from the IRS to the Justice Department or the FBI based on false statements pertaining to political activity?
- Does the FBI have the expertise and resources to investigate cases relating to false statements on IRS forms? If not, what impediments to effective investigation exist?
- In the ongoing investigation of improper targeting of 501(c) tax-exempt groups by the IRS, will the FBI also investigate potential underlying criminal conduct by exempt groups, such as material false statements, where evidence of such misconduct appears?

QUESTIONS SUBMITTED BY SENATOR CHARLES E. GRASSLEY FOR HON. ROBERT S.
MUELLER III

Senate Committee on the Judiciary
Hearing on Oversight of the Federal Bureau of Investigation
June 19, 2013
Questions for the Record from Ranking Member Charles E. Grassley
To Robert Mueller III
Director, Federal Bureau of Investigation

1. Border Patrol Agent Brian Terry Shooting

At the hearing, I asked you if you could put to rest the conspiracy theories out there that the FBI or an FBI informant was out in Peck Canyon before Border Patrol Agent Brian Terry was shot. You stated that you didn't believe there was any truth in those theories, but you wanted to go back and make certain that the FBI doesn't have anything that would be supportive of those theories.

a. In going back, did you uncover anything that would be supportive of those theories? Please describe the process you utilized to make this determination.

2. Knowledge of Terry Shooting Connection to Operation Fast and Furious

At the hearing, I told you I would be submitting a detailed list of questions about a concern the family of Border Patrol Agent Brian Terry has that there was an attempt to cover up the connection between Operation Fast and Furious and the guns found at the scene of his shooting. According to the family, the indications of an attempt to cover up haven't been fully investigated.

Documents produced by the Justice Department in response to the Congressional investigation into Operation Fast and Furious show that then-U.S. Attorney Dennis Burke, along with then-First Assistant U.S. Attorney (AUSA) Ann Scheel, received an e-mail at 5:19 pm on December 15, 2010, from Shelley Clemens. Ms. Clemens was the head of the Tucson office of the U.S. Attorney's Office for the District of the Arizona (USA AZ). Ms. Clemens had attended the Department of Homeland Security's press conference on Agent Terry's death. She apparently spoke with Nathan Gray, the Special Agent in Charge (SAC) of the Federal Bureau of Investigation (FBI) Phoenix Field Office. Ms. Clemens' e-mail to Mr. Burke and Ms. Scheel read: "Nate Grey [sic] was here and advised that the 2 guns are tied to an on-going Phoenix ATF inv. You will probably get a call from Bill Newell."¹ Two hours later, Burke responded: "Thanks. I just talked to Bill Newell about it. The guns tie back to Emory's Fast and Furious case."²

When I asked Secretary Napolitano about visiting Arizona shortly after Agent Terry's shooting, she testified:

When Agent Terry was killed, it was December 14th. I went to Arizona a few days thereafter to meet with the FBI agents and the assistant U.S. attorneys who

¹ E-mail from Shelley Clemens to Dennis Burke and Ann Scheel (Dec. 15, 2010, 5:19 pm) [HOGR DOJ 005917].
² E-mail from Dennis Burke to Shelley Clemens and Ann Scheel (Dec. 15, 2010, 7:21 pm) [HOGR DOJ 005917].

were actually going to look for the shooters. At that time, nobody had done the forensics on the guns and "Fast and Furious" was not mentioned. But I wanted to be sure that those responsible for his death were brought to justice, and that every DOJ resource was being brought to bear on that topic. So I did have conversations in – it would have December of '09 – about the murder of Agent Terry. **But at that point in time, there – nobody knew about "Fast and Furious."**³

The Department of Homeland Security Inspector General report on Operation Fast and Furious also stated that no one informed Secretary Napolitano of the connection during her visit to Arizona.⁴ The Department of Justice Inspector General report failed to address the issue.⁵

It is difficult to understand why the FBI, which informed the U.S. Attorney's Office of the connection, would fail to inform Secretary Napolitano of the connection when she visited Arizona in the days after Brian Terry's murder.

- a. When and how did FBI Special Agent in Charge (SAC) Nathan Gray learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?
- b. When and how did the FBI Assistant Special Agent in Charge (ASAC) in Arizona learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?
- c. When and how did the FBI personnel investigating the Terry murder learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?
- d. Which FBI personnel attended and conducted briefings for Secretary Napolitano and U.S. Customs and Border Protection (CBP) Commissioner Alan Bersin in the days after the Brian Terry murder?
- e. As part of such briefings, did anyone from the FBI brief Commissioner Bersin on the connection of the weapons found at the scene to Fast and Furious? If not, why not?
- f. Why didn't FBI officials inform Secretary Napolitano that the guns at the scene came from Fast and Furious?

³ Testimony of Janet Napolitano before the Senate Committee on the Judiciary, "Oversight of the Department of Homeland Security," October 26, 2011.

⁴ U.S. Department of Homeland Security, Office of the Inspector General, "DHS Involvement in OCDETF Operation Fast and Furious" (Mar. 2013), at 10.

⁵ U.S. Department of Justice, Office of the Inspector General, "A Review of ATF's Operation Fast and Furious and Related Matters" (Sep. 2012), at 289.

- g. Given that the possible murder weapons were linked to an ATF operation, did the FBI give the personnel working the Brian Terry murder any guidance or instruction regarding this connection? If so, please describe the guidance or instruction in detail.
- h. Did Dennis Burke give the FBI any general guidance or instructions the Terry murder investigation and its connection to ATF's Operation Fast and Furious? If so, please describe the guidance or instruction in detail.
- i. Did Dennis Burke advise, request, or instruct the FBI not to talk about the connection between the Terry murder investigation and ATF's Operation Fast and Furious with Congress or any federal, state, or local officials? If so, please describe the communication in detail.
- j. At any time was anyone in the FBI instructed to remain silent about the connection of the weapons to Operation Fast and Furious or to refrain from sharing that information with Congress or any federal, state, or local officials? If so, by whom and please provide a detailed description of the communication.

3. Use of Drones by the FBI

In recent responses to questions I asked Attorney General Holder following his last oversight hearing, the Department of Justice advised this Committee that the Drug Enforcement Administration and the Bureau of Alcohol, Tobacco, and Firearms have acquired Unmanned Aircraft Systems, commonly known as drones.

The Department indicated that these agencies were drawing up plans and procedures for use of drones as well. The responses did not indicate whether the FBI had acquired any drones or whether there were future plans for drone technology use by the FBI. At the hearing, I asked you about the FBI's use of drones and you replied that the FBI currently uses drones in limited circumstances. I would like more information on the use of drones by the FBI and the privacy protections placed on their use.

- a. When did the FBI begin using drones?
- b. When did the FBI first use a drone for a domestic purpose?
- c. How many times has the FBI deployed drones on U.S. soil? Provide dates and locations where drones were utilized.
- d. Does the FBI have an agreement with any other government agency such as the Department of Defense or Department of Homeland Security to receive the assistance of Drones?
- e. Does the FBI have agreements in place with the Department of Defense or Department of Homeland Security, or any other agency, to share drone airframes and/or information obtained based upon drone use?

- f. Has the FBI developed a set of policies, procedures or operational limits on use of drones? If so, who is evaluating the privacy impact on American citizens? If not, why have drones been used before such a policy was in place?
- g. Has the FBI sought certification and/or prior approval for use of drones on U.S. soil with the FAA? If so, when?
- h. How many drones does the FBI currently possess? Please provide make and model information as well as the costs for these systems.
- i. What are the approved uses of drones by FBI agents?
- j. Who must sign off on the use of drones for surveillance on U.S. soil? What about instances where drones are used abroad?
- k. Does the FBI inform the Judicial Branch prior to deployment of drones? If not, why not?
- l. Does the FBI obtain search warrants or other prior judicial approval before deploying drones on U.S. soil?
- m. What limitations are placed on the use of drones?
- n. Are any of the drones utilized by the FBI armed or capable of being armed?
- o. Are any of the drones utilized by the FBI carrying, or capable of carrying, non-lethal weapons?
- p. Has the FBI coordinated drone use and tactics with the DEA and ATF? If not, why not?
- q. Who operates the FBI's drones? Is it a Special Agent trained in search and seizure law, FBI pilot, or another employee of the FBI?
- r. Who at the Department or FBI authorized the use of drones by the FBI?

4. Boston Marathon Bombing

On Monday, April 15, 2013, two bomb blasts rocked the Boston Marathon finish line and initiated a five day investigation and manhunt coordinated by the FBI. Late on Thursday night, the investigation shifted focus to two brothers, Tamerlan and Dzhokhar Tsarnaev. Tamerlan Tsarnaev died in Watertown, MA after a chase with Massachusetts police officers and Dzhokhar was apprehended in the same town the following day.

Following his death, it was revealed that Tamerlan Tsarnaev had been questioned by the FBI in early 2011 at the request of Russia but the case was not pursued further. This, despite the

fact that Tsarnaev traveled to Sheremetyevo, Russia, in January 2012—less than a year after the tip from Russian security services that he was preparing to travel to Russia to join underground group. It was later revealed that in the course of his trip to Russia, during routine surveillance of an individual known to be involved in the militant Islamic underground movement, police witnessed Tamerlan meet the latter at a Salafi mosque in Makhachkala. The travel alone should have raised flags for the FBI, but it is still unclear what was done with the information when the government was notified that he was traveling to Russia.

One of the primary purposes of Joint Terrorism Task Forces is to facilitate communication among federal and state law enforcement. At a hearing with Secretary Janet Napolitano in April of this year, she claimed that when the older of the brothers in the Boston bombing left the country to travel to Russia, “the system pinged.”

In your hearing last week, you stated, “[the] indication that he was on his way back to Russia did not get acted upon,” but that there has been a correction to your procedures.

- a. When the system “pinged” upon the older brother’s exit from this country, did DHS notify the FBI?
 - i. If not, why not? What procedures have been corrected to ensure this does not occur again?
 - ii. If so, when and how did DHS notify FBI and what did the FBI do with that information?

According to the New York Times, of the 22 most alarming plans for attacks since 9/11 on American soil, 14 involved FBI sting operations using undercover agents and informers who pose as terrorists.

- b. You said in a House hearing last week that the FBI agents initially investigating the older brother prior to the Boston bombing used the tools available to him at the time. Did the FBI attempt to use the tactic of ‘recruitment’ or a sting operation with him? If not, why not?
- c. Other than his interview by agents following the warning from Russia, has the FBI had any other contact with the either of the brothers?

It is my understanding that the FBI did not investigate the triple homicide involving one of the bombers friends until learning of a possible connection after the Marathon Bombings. The Massachusetts State Police in Middlesex County were the lead investigative agency in the murder case.

- d. Did Massachusetts State Police Detectives in Middlesex County have the ability to query FBI databases and discover information about the Russia’s warning about the older brother? IF NOT, why not?

- e. Information about the older brother's radicalization might have placed his potential connection to the triple murder in a totally different light. Why didn't the FBI share the information it received from Russia with local authorities through the Joint Terrorism Task Force process?

Following the shootout in which a number of rounds were reported to have been fired by the brothers at police officers and the arrest of the younger brother the following day, initial news reports indicated that as many as three guns were recovered in the course of the investigation and manhunt. Reports were later changed to indicate that only one gun was recovered.

- f. In an effort to clarify the record, how many firearms were recovered that were linked to the investigation?
- g. Are you aware of the reasons for the discrepancy between the reports?

5. FBI Crime Lab

In an oversight hearing thirteen months ago, both Chairman Leahy and I asked you some questions regarding notification of defendants in cases involving faulty FBI crime lab reports. You indicated that you would get back to both of us, and Chairman Leahy and I followed up with a letter on May 21, 2012. However, we did not get a response until December 2012. It did not answer our specific questions about the 1996 review, and no one since then has been willing to provide Chairman Leahy's and my staff with a briefing on that review.

- a. How many problem cases were identified in the 1996 review?
- b. In how many cases was the defendant notified?
- c. Who in FBI or the Justice Department has control of the data produced by the 1996 task force?

6. Change in Immigration Criminal Law

Current law punishes a person who makes an illegal passport or who provides materials for the making of passport. Current law also makes it illegal to use illegal documents. The Immigration Bill S.744 weakens current law by requiring only those who make and distribute illegal passports 3 or more times to be charged with a crime, only those who collect materials that are used for 10 or more passports will be charged with a crime, and the focus of the bill is on the makers of illegal passports, and less so on persons who use illegal documents.

- a. Will these changes to current law have a negative impact on the counterterrorism and counterintelligence efforts of the FBI?

- b. Do you agree that this weakening of current law creates a loophole that could allow terrorist groups, such as Al Qaeda or Hezbollah, or foreign spies to more easily operate within the United States?

7. FBI Whistleblower Case Status

I have repeatedly asked you follow-up questions regarding the current status of two FBI Whistleblower cases working their way through the system. Agent Jane Turner, who initially filed her complaint approximately 9 years ago and has yet to receive a final decision and Robert Kobus who has been waiting for approximately 4 years.

- a. Why has the FBI appealed and fought Special Agent Jane Turner's case for nearly a decade and what action was taken against those persons who participated in the retaliation against Ms. Turner?
- b. What is the current status of Robert Kobus' case, and if there has been a ruling by the Office of Attorney Recruitment and Management, why has my office not been provided a copy?

8. Training Videos and FBI Budget

A June 6 New York Times article revealed that the FBI had hired actor Michael R. Davis. Mr. Davis was used by the Internal Revenue Service in its Mad Men parody training video, which cost taxpayers tens of thousands of dollars.

- a. Has the FBI created any training videos similar to those at the IRS which have received such public attention? If so, how many, and what was the cost of each video?
- b. What was Mr. Davis paid to do for the FBI?
- c. How does this square with the FBI's statements to Congress in the past that it is underfunded?

9. Mark Rossetti

On October 14, 2011, I sent you a letter with questions about the FBI's attempt to hide its relationship with a Boston mobster, Mark Rossetti from the Massachusetts State Police. After initial denials, the FBI finally admitted that it did hide its relationship with this informant from the State Police. The FBI promised a report including recommended policy changes.

It has almost a year since this promise. Mr. Rossetti and over twenty of his associates have pled guilty. I have been informed by sources in Boston that all cases linked to Rossetti are finished. Despite this, there is still no report.

- a. When will the report be ready?

- b. Will you provide it to the Committee?
- c. Have any changes been made to informant policy as a result of this case?

10. Discipline for Prostitution

On September 27, 2012, you sent a letter to the FBI regarding allegations that an undercover agent in the Philippines was ordered prostitutes on multiple occasions himself and other cooperating individuals. Worse, the Government of the Philippines raided one of brothels the prostitutes were allegedly solicited at and rescued 60 victims of human trafficking, 20 of whom were minors.

On April 4, 2013, the FBI provided me with a letter regarding historical information on how the FBI has dealt with prostitution. I was surprised at some of the discipline. For example, one GS-14 supervisory agent obtained inappropriate services at a massage parlor on 10 occasions right here in Washington, D.C. He also committed time and attendance abuse and misused his government vehicle. However, that agent is still an FBI employee. Others here in D.C. also obtained inappropriate services at massage parlors in 2010 and 2012, yet received minor suspensions and are still FBI employees.

- a. Why were employees like these not terminated?

11. Cybersecurity and Information Sharing

Your written testimony points out the ever growing cyber threat to both our government and private industry. You also state that the FBI must “develop channels for sharing information and intelligence quickly and effectively.”

While I applaud the fact the FBI has taken a more proactive role in working with the private sector, there are still gaps that need to be filled. Only when we have a true flow of information, going in both directions, will we be able to mitigate and prevent cyber threats.

- a. Director Mueller, what barriers currently prevent a free flow of information sharing between the government and the private sector?
- b. What incentives can and should be provided to the private sector to encourage information sharing with the government and with other private businesses?
- c. Is legislation required to provide these incentives to the private sector?
- d. Do you agree with General Alexander’s statement last week before the Senate Appropriations Committee that “if the government asks [a] company to do something to protect the networks, or to do something and a mistake is made, and it was our fault, then [the company] should have liability protection for that”?

- e. Should liability protection for companies be conditional? If so, when should it apply and what could cause a company to lose liability protection?
- f. When, if at all, is it appropriate for private companies facing cyber-attacks to use a “defensive countermeasure”? And how would you define that term?

12. DOJ OIG Closed Cases

The Justice Department Office of Inspector General (OIG) conducted an investigation between October 2012 and March 2013 in which an FBI Supervisory Intelligence Analyst (SIA) had co-ownership of a joint business venture with his ex-wife, had jointly purchased or guaranteed several commercial and residential rental properties, and that they had defaulted on a \$4.1 million commercial loan guarantee. The SIA failed to disclose some of these assets and the default on his FBI security and financial disclosure form, and he failed to report in a timely manner that he was named a defendant in a lawsuit related to the default. Prosecution was declined in the case and the OIG provided its Report of Investigation (ROI) to the Office of Professional Responsibility (OPR) for appropriate action.

- a. Did the SIA have the proper paperwork on file authorizing secondary employment?
- b. If so, who authorized this secondary employment?
- c. What was the disciplinary decision issued by the FBI's OPR?
- d. What is this employee's current employment status and assignment?
- e. Did this employee have a security clearance? If so, what level and what is the status of that clearance presently?

The OIG also conducted an investigation between October 2012 and March 2013 in which a FBI Assistant Special Agent in Charge (ASAC) was found to be engaged in a personal relationship with a subordinate. The investigation also revealed that the ASAC willfully ignored a former SAC's instruction to terminate the relationship; that the ASAC and subordinate misused an FBI vehicle and FBI-issued Blackberry devices in furtherance of the relationship; and that the ASAC had given the subordinate gifts and money in violation of FBI policy. The ASAC also failed to disclose the relationship during his FBI security re-investigation. The FBI agent was placed on a 60-day suspension and upon his request, was reassigned to a GS-13 position in the same field office.

- f. How did the two FBI employees misuse the FBI vehicle in this relationship?
- g. Did the FBI provide records for the agents' government issued gas cards to the DOJ OIG?
- h. How did the FBI agents misuse their FBI-issued Blackberry devices?

- i. At what financial cost were the above misuses passed to the taxpayer?
- j. How many FBI agents were found to have misused their FBI-issued Blackberry devices in the same timeframe (October 2012-March 2013)?
- k. Was the female subordinate found to have received any bonuses or financial benefits from the FBI during the timeframe of their relationship?
- l. In what form was the FBI security re-investigation in which the ASAC failed to disclose his relationship done (verbal or written)? Was there ever discussion between the OIG and FBI about prosecuting the ASAC for an 18 USC 1001 charge?

13. Investigation of Former Director of Central Intelligence Petreaus:

Six months ago, I wrote you regarding the resignation of Director of Central Intelligence (DCI) David Petreaus and the involvement by the U.S. Department of Justice (Department), including the Federal Bureau of Investigation (FBI), in uncovering information that revealed an extramarital affair cited by General Petreaus as a reason for his resignation. My letter requested a briefing similar to the one provided to members of the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and Chairman Leahy of the Senate Committee on the Judiciary at that time.

On June 6, 2013, I received a letter from the Department of Justice stating, "Inasmuch as this is an ongoing investigation and significant individual privacy interests are implicated, we are unable to provide you with a briefing or provide answers to...your letter." Aside from the issue that the Chairman of the Judiciary *was* provided a briefing despite the reasons listed above while I was not, it is my understanding that there were two investigative inquiries being conducted regarding the Petreus matter. One inquiry was criminal while the other pertained to matters of National Security.

It is my understanding that the investigation regarding National Security is still ongoing. However, based upon the declination letter sent to Paula Broadwell in December and the statement of Department spokesman William C. Daniels, it appears that the criminal case is closed. According to Daniels, "After applying relevant case law to the particular facts of this case, the United States Attorney's Office for the Middle District of Florida has decided not to pursue a federal case regarding the alleged acts of 'cyber-stalking' involving Paula Broadwell." Inasmuch as it appears the criminal case is closed, I resubmit my requests regarding the *criminal* matter once again. Please provide:

- a. a timeline of events from initial contact with FBI personnel through the close of the criminal inquiry;
- b. an explanation of how and why the FBI opened the criminal inquiry;
- c. a detailed list of personnel who signed off on the criminal investigation;

- d. a detailed account of the legal authorities used to obtain each of the electronic communications of those involved including NSLs and Exigent Letters, and the role, if any, of any U.S. Attorneys' Offices;
- e. an explanation of the timing and circumstances of how you first learned of this criminal inquiry and when the White House was notified of the inquiry;
- f. a description of Department employees' contacts with Congress prior to the election and whether the Department considers those contacts protected whistleblower disclosures;
- g. an explanation of whether the FBI shared information regarding the criminal investigation with investigators or protective security details from various military criminal investigation organizations (including the CIA, Army Criminal Investigation Command (CID), Air Force Office of Special Investigations (OSI), or Navy Criminal Investigative Service (NCIS)) and when that information was shared;
- h. a description of the status of any related reviews being conducted by the FBI Inspections Division, the Office of Professional Responsibility, the Deputy Attorney General's Office, or the Office of Inspector General, including any related to public reports of alleged communications between an FBI agent and any witnesses that involved inappropriate photographs or text;
- i. an explanation of whether the extramarital affair was uncovered during the initial background investigation conducted by the FBI prior to General Petraeus' confirmation as DCI;

(10) an explanation of any legal analysis conducted by any component of the Department, including the FBI, regarding whether you or the FBI Director were obligated by law to report the investigation of DCI Petraeus to the President or any other government official.

14. Position on Marijuana Legalization

I understand that enforcing the Controlled Substances Act is not the primary mission of the Federal Bureau of Investigation. However, the FBI does have the authority to investigate drugs and drug trafficking and enforce the Controlled Substances Act.

As you may be aware the states of Colorado and Washington recently passed ballot measures that legalize the possession of small amounts of marijuana for recreational use. These ballot measures are in direct conflict with the Controlled Substances Act.

- a. Do you believe the Controlled Substances Act should be enforced?
- b. Do you support the legalization of marijuana for recreational or any other use?
- c. What do you believe the impact of marijuana legalization is?

15. Housing and Urban Development PHA's

Over the past three years, I have sent numerous letters of inquiry to HUD raising concerns about wasteful spending and possible criminal activity at the PHAs across the country. The FBI has investigated fraud and theft of funds by top housing authority executives, managers and even Board members who have used the funds to pad their own pockets, reward their friends and family, and pay off others to look the other way.

These investigations have been vital for identifying employees who are abusing the public trust and halting further abuse of federal dollars. While I do not want to interfere with ongoing criminal investigations, I believe that this information must be available to the general public, not just the media, to bring greater transparency to how taxpayer dollars are being spent. Therefore, I am requesting the following information:

- a. What agreement(s) is(are) in effect between HUD and the FBI that dictate when the FBI may begin a criminal investigation? Please provide a copy of the agreement(s).
- b. What criteria are required for the FBI to conduct a criminal investigation at a public housing authority?
- c. Please provide a list of the housing authorities the FBI has investigated during the previous five years, as well as the disposition for each.
- d. Please document the housing authorities the FBI declined to investigate and why.

QUESTIONS SUBMITTED BY SENATOR ORRIN G. HATCH FOR HON. ROBERT S. MUELLER
III**Question For The Record For FBI Director Mueller – Senator Hatch**

On May 8, 2013, Senator Whitehouse and Senator Graham convened the Subcommittee on Crime and Terrorism for a hearing on cyber activities by foreign actors. During that hearing, a leading expert on malicious cyber activity testified that only 10-20% of all cyber hacks are state sponsored. This is further corroborated by a February, 2013 report by Trustwave Security that concluded 96% of data breaches are orchestrated by criminals and not state sponsors.

I am worried that we are not effectively using our resources in investigating cybercrime. While I support the FBI's focus on state sponsored activity, it appears that the organization is spending precious budget resources duplicating an already existing electronic crimes task force model which was established 12 years ago in law and is managed by DHS. The long standing electronic crime task forces already have a global footprint, and work with international partners on criminal cyber cases. They've had numerous successes both domestically and internationally due to long standing collaborative efforts with law enforcement, private sector, and academic partners.

The FBI should focus on the state sponsor threat along with curtailing the cyber theft of intellectual property and trade secrets without chilling criminal investigations into cyber hacks and data breaches conducted by cybercriminals with no association to a state sponsor. How does the FBI cooperate with its federal and state partners on non-state sponsored cyber activities?

RESPONSES OF HON. ROBERT S. MUELLER III TO QUESTIONS SUBMITTED BY SENATORS
WHITEHOUSE, GRASSLEY, AND HATCH

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the June 19, 2013, Hearing Before the
Senate Committee on the Judiciary
Regarding "Oversight of the FBI"**

Questions Posed by Senator Whitehouse

1. In response to a question from Senator Durbin, you described the upgrades made to FBI computer systems during your tenure. You also noted that the federal contracting process, in which five-year contracts are common, made it a challenge to adapt to rapidly emerging and changing technologies. In light of those comments please specify the contracting provisions that make it a challenge to adapt rapidly to emerging and changing technologies.

Response:

The FBI receives annual and sometimes incremental funding, which can require that we stage major IT procurement projects in multi-segmented phases. This complicates our ability to update existing IT capabilities or adopt new capabilities, because major IT acquisitions are often multi-year projects. Funding major, multi-year capital investments on a year-to-year basis with a budget that depends on receiving additional funding over multiple fiscal years leads to the possibility that certain operations, divisions, or activities will outpace others in terms of technological upgrades. It is sometimes difficult to develop an efficient plan for updating IT capabilities when this must be done in multiple phases and in competition with other FBI funding priorities. As is the case with all federal agencies and departments, IT contracts are further complicated when we operate during part of the year under a Continuing Resolution that restricts funding availability.

2. At a hearing of the Subcommittee on Crime and Terrorism on April 9, 2013 on "Current Issues in Campaign Finance Law Enforcement," the Subcommittee examined a pattern of what appear to be material false statements made to the government by 501(c)(4) organizations and organizations seeking 501(c)(4) status. These apparent false statements, which pertain to how much political activity the organizations have engaged in or plan to engage in, were made on IRS forms 1024 (application for exempt status), and 990 (return of exempt organization). On first impression, these false statements would seem to violate both 18 U.S.C. § 1001 (false statements) and 2 U.S.C. § 7206 (fraud and false statements made under penalty of perjury).

These responses are current as of 8/26/13

Both the Department of Justice and the IRS have suggested that the Justice Department, and presumably the FBI, would not take an active role in investigating these apparent false statements until specific cases were referred by IRS to the Justice Department. This is in spite of the fact that 18 U.S.C. § 1001 false statement cases are, as Acting Assistant Attorney General for the Criminal Division Mythili Raman described them, “bread-and-butter” cases that investigators and prosecutors handle on a regular basis. Meanwhile, as a number of witnesses and experts have stated, the IRS is ill-equipped to investigate these cases. Neither the Justice Department nor the IRS was able to provide examples of any referrals having been made.

a. Is it the case that the FBI does not investigate apparent criminal false statements on IRS forms absent a referral from the IRS, even where the apparent misconduct is already in the public record (such as through news accounts)? If so, what is the basis for this policy?

Response:

The FBI does not routinely initiate these types of investigations based upon news reports. Instead, we receive referrals from the agencies with regulatory or enforcement authorities, which are in the best position to assess the facts and provide them to the FBI for investigative follow up. In the alternative, if, through the course of an existing investigation or assessment, the FBI receives information indicating a possible criminal violation, we would investigate that matter pursuant to our ordinary investigative authorities and procedures.

b. Are you aware of any referrals from the IRS to the Justice Department or the FBI based on false statements pertaining to political activity?

Response:

The FBI is not aware of any referrals from the IRS to the Department of Justice (DOJ) or the FBI regarding false statements pertaining to political activity.

c. Does the FBI have the expertise and resources to investigate cases relating to false statements on IRS forms? If not, what impediments to effective investigation exist?

d. In the ongoing investigation of improper targeting of 501(c) tax-exempt groups by the IRS, will the FBI also investigate potential underlying criminal conduct by exempt groups, such as material false statements, where evidence of such misconduct appears?

Response to subparts c and d:

These responses are current as of 8/26/13

While the IRS does have the authority to investigate this potential criminal conduct, the FBI would be able to assist on a case-by-case basis if the IRS were to request FBI assistance.

Questions Posed by Senator Grassley

3. At the hearing, I asked you if you could put to rest the conspiracy theories out there that the FBI or an FBI informant was out in Peck Canyon before Border Patrol Agent Brian Terry was shot. You stated that you didn't believe there was any truth in those theories, but you wanted to go back and make certain that the FBI doesn't have anything that would be supportive of those theories. In going back, did you uncover anything that would be supportive of those theories? Please describe the process you utilized to make this determination.

Response:

In October 2011, senior FBI officials briefed your Congressional staff regarding FBI events related to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) operation called Fast and Furious. In that briefing, your staff was explicitly advised that neither the FBI nor any FBI informant was at the scene of Brian Terry's murder and that there was no truth to this conspiracy theory. Nothing has changed in this regard since that briefing.

4. At the hearing, I told you I would be submitting a detailed list of questions about a concern the family of Border Patrol Agent Brian Terry has that there was an attempt to cover up the connection between Operation Fast and Furious and the guns found at the scene of his shooting. According to the family, the indications of an attempt to cover up haven't been fully investigated.

Documents produced by the Justice Department in response to the Congressional investigation into Operation Fast and Furious show that then-U.S. Attorney Dennis Burke, along with then-First Assistant U.S. Attorney (AUSA) Ann Scheel, received an e-mail at 5:19 pm on December 15, 2010, from Shelley Clemens. Ms. Clemens was the head of the Tucson office of the U.S. Attorney's Office for the District of the Arizona (USA AZ). Ms. Clemens had attended the Department of Homeland Security's press conference on Agent Terry's death. She apparently spoke with Nathan Gray, the Special Agent in Charge (SAC) of the Federal Bureau of Investigation (FBI) Phoenix Field Office. Ms. Clemens' e-mail to Mr. Burke and Ms. Scheel read: "Nate Grey [sic] was here and advised that the 2 guns are tied to an on-going Phoenix ATF inv. You will probably get a call from Bill

These responses are current as of 8/26/13

Newell.”¹ Two hours later, Burke responded: “Thanks. I just talked to Bill Newell about it. The guns tie back to Emory’s Fast and Furious case.”²

When I asked Secretary Napolitano about visiting Arizona shortly after Agent Terry’s shooting, she testified:

When Agent Terry was killed, it was December 14th, I went to Arizona a few days thereafter to meet with the FBI agents and the assistant U.S. attorneys who were actually going to look for the shooters. At that time, nobody had done the forensics on the guns and “Fast and Furious” was not mentioned. But I wanted to be sure that those responsible for his death were brought to justice, and that every DOJ resource was being brought to bear on that topic. So I did have conversations in – it would have December of ‘09 – about the murder of Agent Terry. But at that point in time, there – nobody knew about “Fast and Furious.”³

The Department of Homeland Security Inspector General report on Operation Fast and Furious also stated that no one informed Secretary Napolitano of the connection during her visit to Arizona.⁴ The Department of Justice Inspector General report failed to address the issue.⁵

It is difficult to understand why the FBI, which informed the U.S. Attorney’s Office of the connection, would fail to inform Secretary Napolitano of the connection when she visited Arizona in the days after Brian Terry’s murder.

a. When and how did FBI Special Agent in Charge (SAC) Nathan Gray learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?

b. When and how did the FBI Assistant Special Agent in Charge (ASAC) in Arizona learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?

c. When and how did the FBI personnel investigating the Terry murder learn of the connection between an ATF investigation and the guns found at the murder scene of Brian Terry?

¹ E-mail from Shelley Clemens to Dennis Burke and Ann Scheel (Dec. 15, 2010, 5:19 pm) [HOGR DOJ 005917].

² E-mail from Dennis Burke to Shelley Clemens and Ann Scheel (Dec. 15, 2010, 7:21 pm) [HOGR DOJ 005917].

³ Testimony of Janet Napolitano before the Senate Committee on the Judiciary, “Oversight of the Department of Homeland Security,” October 26, 2011.

⁴ U.S. Department of Homeland Security, Office of the Inspector General, “DHS Involvement in OCDETF Operation Fast and Furious” (Mar. 2013), at 10.

⁵ U.S. Department of Justice, Office of the Inspector General, “A Review of ATF’s Operation Fast and Furious and Related Matters” (Sep. 2012), at 289.

These responses are current as of 8/26/13

- d. Which FBI personnel attended and conducted briefings for Secretary Napolitano and U.S. Customs and Border Protection (CBP) Commissioner Alan Bersin in the days after the Brian Terry murder?
- e. As part of such briefings, did anyone from the FBI brief Commissioner Bersin on the connection of the weapons found at the scene to Fast and Furious? If not, why not?
- f. Why didn't FBI officials inform Secretary Napolitano that the guns at the scene came from Fast and Furious?
- g. Given that the possible murder weapons were linked to an ATF operation, did the FBI give the personnel working the Brian Terry murder any guidance or instruction regarding this connection? If so, please describe the guidance or instruction in detail.
- h. Did Dennis Burke give the FBI any general guidance or instructions the Terry murder investigation and its connection to ATF's Operation Fast and Furious? If so, please describe the guidance or instruction in detail.
- i. Did Dennis Burke advise, request, or instruct the FBI not to talk about the connection between the Terry murder investigation and ATF's Operation Fast and Furious with Congress or any federal, state, or local officials? If so, please describe the communication in detail.
- j. At any time was anyone in the FBI instructed to remain silent about the connection of the weapons to Operation Fast and Furious or to refrain from sharing that information with Congress or any federal, state, or local officials? If so, by whom and please provide a detailed description of the communication.

Response to subparts a through j:

When the FBI was assigned to investigate the murder of U.S. Customs and Border Protection (CBP) Agent Terry, the early focus of this investigation was on the identity of the shooter(s) and not on the origin of the weapons used. As has been investigated by DOJ's Office of the Inspector General (OIG) and explained in the September 2012 OIG report (re-issued in November 2012), the FBI was not responsible for determining whether errors in ATF's investigation led to the presence of Fast and Furious weapons at the murder scene. The OIG investigation does not indicate, and we are not aware of any information supporting, any knowledge by the FBI of a link between Agent Terry's murder and ATF's Operation Fast and Furious before this linkage was widely reported.

These responses are current as of 8/26/13

5. In recent responses to questions I asked Attorney General Holder following his last oversight hearing, the Department of Justice advised this Committee that the Drug Enforcement Administration and the Bureau of Alcohol, Tobacco, and Firearms have acquired Unmanned Aircraft Systems, commonly known as drones.

The Department indicated that these agencies were drawing up plans and procedures for use of drones as well. The responses did not indicate whether the FBI had acquired any drones or whether there were future plans for drone technology use by the FBI. At the hearing, I asked you about the FBI's use of drones and you replied that the FBI currently uses drones in limited circumstances. I would like more information on the use of drones by the FBI and the privacy protections placed on their use.

- a. When did the FBI begin using drones?
- b. When did the FBI first use a drone for a domestic purpose?
- c. How many times has the FBI deployed drones on U.S. soil? Provide dates and locations where drones were utilized.
- d. Does the FBI have an agreement with any other government agency such as the Department of Defense or Department of Homeland Security to receive the assistance of Drones?
- e. Does the FBI have agreements in place with the Department of Defense or Department of Homeland Security, or any other agency, to share drone airframes and/or information obtained based upon drone use?
- f. Has the FBI developed a set of policies, procedures or operational limits on use of drones? If so, who is evaluating the privacy impact on American citizens? If not, why have drones been used before such a policy was in place?
- g. Has the FBI sought certification and/or prior approval for use of drones on U.S. soil with the FAA? If so, when?
- h. How many drones does the FBI currently possess? Please provide make and model information as well as the costs for these systems.
- i. What are the approved uses of drones by FBI agents?
- j. Who must sign off on the use of drones for surveillance on U.S. soil? What about instances where drones are used abroad?

These responses are current as of 8/26/13

k. Does the FBI inform the Judicial Branch prior to deployment of drones? If not, why not?

l. Does the FBI obtain search warrants or other prior judicial approval before deploying drones on U.S. soil?

m. What limitations are placed on the use of drones?

n. Are any of the drones utilized by the FBI armed or capable of being armed?

o. Are any of the drones utilized by the FBI carrying, or capable of carrying, non-lethal weapons?

p. Has the FBI coordinated drone use and tactics with the DEA and ATF? If not, why not?

q. Who operates the FBI's drones? Is it a Special Agent trained in search and seizure law, FBI pilot, or another employee of the FBI?

r. Who at the Department or FBI authorized the use of drones by the FBI?

Response to subparts a through r:

As we briefed Senate Judiciary Committee staff on July 12, 2013, the FBI uses Unmanned Aircraft Systems (UAS) in limited circumstances when there is a specific, operational need. UAS have been used for surveillance to support missions related to kidnappings, search and rescue operations, drug interdictions, and fugitive investigations. The FBI has conducted surveillance using UAS in eight criminal cases and two national security cases. For example, in 2013 in Alabama, the FBI used UAS surveillance to support the successful rescue of the 5-year-old child who was being held hostage in an underground bunker by Jimmy Lee Dykes. None of the UAS used by the FBI are armed with either lethal or non-lethal weapons, and the FBI has no plans to use weapons with UAS. The FBI does not use UAS to conduct "bulk" surveillance or to conduct general surveillance not related to a specific investigation or assessment.

The FBI only conducts UAS surveillance consistent with Department and FBI rules and regulations for conducting aerial surveillance in our investigations. Specifically, the FBI's use of UAS for surveillance is governed by: the Fourth Amendment of the United States Constitution and Federal laws and policies including the Privacy Act; Federal Aviation Administration (FAA) rules and regulations; the Attorney General Guidelines for Domestic FBI Operations; the FBI's Domestic Investigations and Operations Guide (DIOG) and the FBI's 2011 Bureau Aviation Regulations Manual (BAR), which has

These responses are current as of 8/26/13

specific policies for the use of UAS for aerial surveillance. For example, the FBI must obtain a Certificate of Authorization (COA) from the FAA prior to using UAS for surveillance, and must comply with the FAA's guidelines on the use of UAS in the national airspace (this includes significant limits on the area where and altitude at which UAS can be operated). *See* FAA Interim Operational Approval Guidance, UAS Policy 05-01, "Unmanned Aircraft Systems: Operations in the U.S. National Airspace System" (2008).

Prior to FBI deploying UAS, every request to use UAS for surveillance must also be approved by FBI management at FBI Headquarters and in the relevant FBI Field Office. In addition, requests to use UAS for surveillance are reviewed by FBI legal counsel where there is a belief that an individual may have a reasonable expectation of privacy under the Fourth Amendment. This review is designed to ensure that the proposed use of UAS is consistent with the Fourth Amendment, and that the required privacy and civil liberties analysis is conducted prior to deployment of the UAS. The FBI will not use UAS to acquire information in circumstances in which individuals have a reasonable expectation of privacy except, as is true in non-UAS circumstances, where a warrant has been obtained or an exception to the warrant requirement of the Fourth Amendment exists. To date, there has been no need for the FBI to seek a search warrant or judicial order in any of the few cases where UAS have been used.

6. On Monday, April 15, 2013, two bomb blasts rocked the Boston Marathon finish line and initiated a five day investigation and manhunt coordinated by the FBI. Late on Thursday night, the investigation shifted focus to two brothers, Tamerlan and Dzhokhar Tsarnaev. Tamerlan Tsarnaev died in Watertown, MA after a chase with Massachusetts police officers and Dzhokhar was apprehended in the same town the following day.

Following his death, it was revealed that Tamerlan Tsarnaev had been questioned by the FBI in early 2011 at the request of Russia but the case was not pursued further. This, despite the fact that Tsarnaev traveled to Sheremetyevo, Russia, in January 2012—less than a year after the tip from Russian security services that he was preparing to travel to Russia to join underground group. It was later revealed that in the course of his trip to Russia, during routine surveillance of an individual known to be involved in the militant Islamic underground movement, police witnessed Tamerlan meet the latter at a Salafi mosque in Makhachkala. The travel alone should have raised flags for the FBI, but it is still unclear what was done with the information when the government was notified that he was traveling to Russia.

One of the primary purposes of Joint Terrorism Task Forces is to facilitate communication among federal and state law enforcement. At a hearing with Secretary Janet Napolitano in April of this year, she claimed that when the older of the brothers in the Boston bombing left the country to travel to Russia, "the system pinged."

These responses are current as of 8/26/13

In your hearing last week, you stated, “[the] indication that he was on his way back to Russia did not get acted upon,” but that there has been a correction to your procedures.

- a. When the system “pinged” upon the older brother’s exit from this country, did DHS notify the FBI?**
- b. If not, why not? What procedures have been corrected to ensure this does not occur again?**
- c. If so, when and how did DHS notify FBI and what did the FBI do with that information?**

Response to subparts a through c:

At the request of the FBI case agent assessing information about Tamerlan Tsarnaev (hereafter Tamerlan), the CBP Task Force Officer assigned to the Boston Joint Terrorism Task Force (JTF) created a record in the Department of Homeland Security (DHS) TECS System regarding Tamerlan. The CBP Task Force Officer received notification of Tamerlan’s outbound travel in January 2012, approximately seven months after the JTF’s Guardian assessment of Tamerlan was closed. No further investigative steps were taken by the JTF in response to this notification. While there is no record indicating that the CBP Task Force Officer notified the FBI case agent who handled the Guardian assessment of Tamerlan, such notifications were often made informally among JTF members. Since the Boston Marathon bombing, procedures have been revised so that, if this situation were to occur now, the CBP Task Force Officer would formally notify the FBI case agent of Tamerlan’s travel to or from the United States.

- 7. According to the New York Times, of the 22 most alarming plans for attacks since 9/11 on American soil, 14 involved FBI sting operations using undercover agents and informers who pose as terrorists.**

- a. You said in a House hearing last week that the FBI agents initially investigating the older brother prior to the Boston bombing used the tools available to him at the time. Did the FBI attempt to use the tactic of ‘recruitment’ or a sting operation with him? If not, why not?**

Response:

The FBI’s Domestic Investigations and Operations Guide (DIOG) delineates the criteria required for opening the various types of FBI inquiries. Depending on the amount and

These responses are current as of 8/26/13

type of predication established, different techniques and different levels of intrusiveness are authorized.

In the case of Tamerlan, the information available to the FBI in 2011 supported the opening of only an assessment, and not a predicated investigation. An assessment requires no particular factual predication, but does require an authorized purpose and clearly defined objective. The use of undercover techniques is authorized only for predicated investigations. Accordingly, the FBI did not use an undercover technique during the assessment of Tamerlan. The FBI did not attempt to "recruit" Tamerlan because the information available to the FBI at the time did not indicate that he would be able to identify other individuals or groups who may pose a threat to national security.

b. Other than his interview by agents following the warning from Russia, has the FBI had any other contact with the either of the brothers?

Response:

The FBI had no contact with the Tsarnaev brothers between the closing of the Guardian assessment and the events following the Boston Marathon bombing.

8. It is my understanding that the FBI did not investigate the triple homicide involving one of the bombers friends until learning of a possible connection after the Marathon Bombings. The Massachusetts State Police in Middlesex County were the lead investigative agency in the murder case.

a. Did Massachusetts State Police Detectives in Middlesex County have the ability to query FBI databases and discover information about the Russia's warning about the older brother? IF NOT, why not?

b. Information about the older brother's radicalization might have placed his potential connection to the triple murder in a totally different light. Why didn't the FBI share the information it received from Russia with local authorities through the Joint Terrorism Task Force process?

Response to subparts a and b:

The Massachusetts State Police, which continues to be the lead investigative agency for the triple homicide in Waltham, Massachusetts, is a member of the local JTTF. All state and local task force officers on the JTTF have access to the FBI's databases, which contain the Guardian assessment of Tamerlan.

These responses are current as of 8/26/13

9. Following the shootout in which a number of rounds were reported to have been fired by the brothers at police officers and the arrest of the younger brother the following day, initial news reports indicated that as many as three guns were recovered in the course of the investigation and manhunt. Reports were later changed to indicate that only one gun was recovered.

a. In an effort to clarify the record, how many firearms were recovered that were linked to the investigation?

Response:

The number of guns recovered in the aftermath of the Boston Marathon bombing is a part of the criminal investigation of the bombing. Longstanding DOJ policy generally precludes the FBI from disclosing nonpublic information about ongoing investigations.

b. Are you aware of the reasons for the discrepancy between the reports?

Response:

The FBI is not in a position to comment on information reported by news agencies unless it was based on an FBI press release or public comment. Such questions are best posed to the news outlets that disseminated the information.

10. In an oversight hearing thirteen months ago, both Chairman Leahy and I asked you some questions regarding notification of defendants in cases involving faulty FBI crime lab reports. You indicated that you would get back to both of us, and Chairman Leahy and I followed up with a letter on May 21, 2012. However, we did not get a response until December 2012. It did not answer our specific questions about the 1996 review, and no one since then has been willing to provide Chairman Leahy's and my staff with a briefing on that review.

a. How many problem cases were identified in the 1996 review?

b. In how many cases was the defendant notified?

c. Who in FBI or the Justice Department has control of the data produced by the 1996 task force?

Response to subparts a through c:

These responses are current as of 8/26/13

DOJ, which is responsible for this review, provided a briefing for Committee Staff on September 27, 2013.⁶

11. Current law punishes a person who makes an illegal passport or who provides materials for the making of passport. Current law also makes it illegal to use illegal documents. The Immigration Bill S.744 weakens current law by requiring only those who make and distribute illegal passports 3 or more times to be charged with a crime, only those who collect materials that are used for 10 or more passports will be charged with a crime, and the focus of the bill is on the makers of illegal passports, and less so on persons who use illegal documents.

a. Will these changes to current law have a negative impact on the counterterrorism and counterintelligence efforts of the FBI?

b. Do you agree that this weakening of current law creates a loophole that could allow terrorist groups, such as Al Qaeda or Hezbollah, or foreign spies to more easily operate within the United States?

Response to subparts a and b:

We are aware that S. 744 passed the Senate on June 27, 2013. The FBI typically provides its views of pending legislation to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position, and the Administration has already publicly stated its views of S.744.

12. I have repeatedly asked you follow-up questions regarding the current status of two FBI Whistleblower cases working their way through the system. Agent Jane Turner, who initially filed her complaint approximately 9 years ago and has yet to receive a final decision and Robert Kobus who has been waiting for approximately 4 years.

a. Why has the FBI appealed and fought Special Agent Jane Turner's case for nearly a decade and what action was taken against those persons who participated in the retaliation against Ms. Turner?

Response:

Both sides filed appeals in this case, but the matter has now been fully resolved. DOJ's Office of Attorney Recruitment and Management (OARM) had initially ruled in favor of Ms. Turner in May 2010. Among other things, the FBI appealed OARM's conclusion that Ms. Turner had retired involuntarily and was therefore entitled to back pay. The

⁶ Although these responses are, as a whole, current as of 8/26/13, we have updated this sole response to reflect this 9/27/13 activity.

These responses are current as of 8/26/13

matter was remanded to OARM for reconsideration under the correct legal standard. On remand, OARM agreed with the FBI that Ms. Turner had retired voluntarily and was not entitled to back pay. Ms. Turner appealed this decision, which the Deputy Attorney General affirmed. The Deputy Attorney General issued a Final Corrective Action Order (FCAO) on January 12, 2013. The FCAO required the removal of specified items from Ms. Turner's personnel file and the payment of attorneys' fees. The FBI has complied with the FCAO. The Office of the Deputy Attorney General formally closed the case on July 1, 2013. The matter resulted in no disciplinary action because pertinent FBI employees had retired by the time of the final decision.

b. What is the current status of Robert Kobus' case, and if there has been a ruling by the Office of Attorney Recruitment and Management, why has my office not been provided a copy?

Response:

DOJ's OARM issued a decision on the substantive merits of Mr. Kobus' reprisal claims on February 13, 2013. Within days of OARM's decision, the FBI paid to Mr. Kobus the back pay ordered by OARM. At the time of OARM's decision, Mr. Kobus was already in a supervisory position, as required by the OARM decision. OARM's decision left open for further proceedings a number of other issues, including medical costs, the availability of compensatory damages, and attorneys' fees. OARM directed the submission of additional evidence and legal briefs on these issues, and these issues remain pending before OARM.

13. A June 6 New York Times article revealed that the FBI had hired actor Michael R. Davis. Mr. Davis was used by the Internal Revenue Service in its Mad Men parody training video, which cost taxpayers tens of thousands of dollars.

a. Has the FBI created any training videos similar to those at the IRS which have received such public attention? If so, how many, and what was the cost of each video?

b. What was Mr. Davis paid to do for the FBI?

c. How does this square with the FBI's statements to Congress in the past that it is underfunded?

Response to subparts a through c:

The FBI's Training Division, which develops video and other training programs both for Training Division use and for the use of the FBI's other divisions, is the most likely FBI entity to employ actors in training programs. Although historically we have not centrally

These responses are current as of 8/26/13

tracked all of the FBI's training activities, neither the Training Division nor its video production contractor, Rocket Media Group, has ever hired Michael R. Davis for any FBI project.

According to the New York Times article referenced in the question, the "Mad Men" parody was a 4.5-minute video produced by the IRS that "reaches deep for art-world metaphors to describe how I.R.S. employees can assist confused taxpayers." The FBI has not produced training videos "similar" to this description. We have, however, produced two substantive training videos that use humor to teach serious topics.

The first, entitled, "Procurement Integrity Awareness for Executives and Managers," was created in 2008 and uses a combination of video and computer training to provide managerial personnel who may become involved in the procurement process with substantive instruction on a variety of related topics. The video portion of the training, which is 36 minutes in length, is centered on a parody of the "Twilight Zone" and is called "The Ethics Zone." This video is available online to all FBI personnel but is mandatory each year for FBI managerial personnel. The production begins with an introduction by former DOJ Inspector General Glenn Fine and takes about an hour to complete. The video portion cost approximately \$35,000 to produce.

The second production, called "The Squad," was completed in 2010, consists entirely of video, and is over one hour in length. It, too, takes a humorous approach to a serious subject: ethics and the standards of conduct. Pursuant to U.S. Office of Government Ethics (OGE) regulations, new employees are to receive ethics materials and one hour of duty time to review them; public filers are to receive one hour of verbal training annually that includes the Standards of Conduct; and "other employees," including confidential disclosure filers, are to receive one hour of verbal training every 3 years and in the interim years a sufficient amount of time to review written training. Although the training for public filers and "other employees" is not mandatory for all employees, as a matter of practice the vast majority of FBI employees receive this training because all employees are required to participate in annual "all division" training sessions at which ethics/Standards training is presented. As noted above, some of this training is presented "live" by qualified instructors, but not all of the FBI's 35,000 employees can attend the scheduled sessions and instructors cannot be sent to all locations around the nation and the world where FBI employees are stationed. To supplement the live training, the FBI employs a variety of training aides, including the FBI-specific video called "The Squad," which is available to all employees online. This training film uses a parody of the popular television show, "The Office" to cover a number of ethics/Standards subjects ranging from the acceptance of gifts from outside sources to the use of Government vehicles. The central character, however, is straight-forward and stresses repeatedly the need to seek advice from ethics counselors whenever an employee is confronted with a questionable situation. This production cost approximately \$126,000, primarily because

These responses are current as of 8/26/13

it uses a number of actors for its many vignettes. In 2011 the FBI received an “Excellence in Innovation Award” which was, in part, for this production.

Both of these training productions have been used continuously since they were created and we anticipate using both for many more years to come. As noted above, we do not believe either of these productions is “similar to” the questioned IRS “Mad Men” parody. We would be pleased to share these videos with the Committee.

14. On October 14, 2011, I sent you a letter with questions about the FBI's attempt to hide its relationship with a Boston mobster, Mark Rossetti from the Massachusetts State Police. After initial denials, the FBI finally admitted that it did hide its relationship with this informant from the State Police. The FBI promised a report including recommended policy changes.

It has almost a year since this promise. Mr. Rossetti and over twenty of his associates have pled guilty. I have been informed by sources in Boston that all cases linked to Rossetti are finished. Despite this, there is still no report.

a. When will the report be ready?

Response:

The FBI's investigation is ongoing. At this time, there is pending litigation in the Commonwealth of Massachusetts that may impact the FBI's investigation. Once these state-level matters have been adjudicated, the FBI's investigation will be completed.

b. Will you provide it to the Committee?

Response:

Upon completion of the investigation, the FBI would be pleased to brief the results to the Committee.

c. Have any changes been made to informant policy as a result of this case?

Response:

This investigation has contributed to ongoing efforts to ensure comprehensive oversight of the FBI's Confidential Human Source (CHS) Program. The FBI's CHS Program is under continual review and has already undergone policy changes that include the following: a change in the authority level required to reopen a CHS who was closed for cause; a change in the authority level and oversight required to operate a CHS who has

These responses are current as of 8/26/13

engaged in unauthorized illegal activity; and guidance regarding the detection and recognition of suspicious behavior patterns in a CHS. (These CHS Program policy changes do not necessarily pertain to this investigation.)

15. On September 27, 2012, you sent a letter to the FBI regarding allegations that an undercover agent in the Philippines was ordered prostitutes on multiple occasions himself and other cooperating individuals. Worse, the Government of the Philippines raided one of brothels the prostitutes were allegedly solicited at and rescued 60 victims of human trafficking, 20 of whom were minors.

On April 4, 2013, the FBI provided me with a letter regarding historical information on how the FBI has dealt with prostitution. I was surprised at some of the discipline. For example, one GS-14 supervisory agent obtained inappropriate services at a massage parlor on 10 occasions right here in Washington, D.C. He also committed time and attendance abuse and misused his government vehicle. However, that agent is still an FBI employee. Others here in D.C. also obtained inappropriate services at massage parlors in 2010 and 2012, yet received minor suspensions and are still FBI employees.

Why were employees like these not terminated?

Response:

Our April 4, 2013 response demonstrates that the FBI takes strong, decisive disciplinary action against employees who engage in sexual misconduct. Although this disciplinary action includes dismissal in appropriate cases, not every case involving sexual misconduct warrants dismissal. In those cases in which we do not dismiss the employee, we nevertheless impose significant disciplinary sanctions. For example, in the case of the GS-14 supervisory agent you cite above, the employee in question received a 60-day suspension, our strongest sanction short of dismissal. A 60-day suspension represents the loss of one-sixth of an employee's annual salary and also means that the employee will not be considered for promotion for at least three years.

17. The Justice Department Office of Inspector General (OIG) conducted an investigation between October 2012 and March 2013 in which an FBI Supervisory Intelligence Analyst (SIA) had co-ownership of a joint business venture with his ex-wife, had jointly purchased or guaranteed several commercial and residential rental properties, and that they had defaulted on a \$4.1 million commercial loan guarantee. The SIA failed to disclose some of these assets and the default on his FBI security and financial disclosure form, and he failed to report in a timely manner that he was named a defendant in a lawsuit related to the default. Prosecution was declined in the case and the OIG provided its Report of Investigation (ROI) to the Office of Professional Responsibility (OPR) for appropriate action.

These responses are current as of 8/26/13

a. Did the SIA have the proper paperwork on file authorizing secondary employment?

b. If so, who authorized this secondary employment?

Response to subparts a and b:

The investigation by DOJ's OIG did not disclose whether the Supervisory Intelligence Analyst (SIA) had reported "outside employment" related to the SIA's joint ownership of a business venture.

c. What was the disciplinary decision issued by the FBI's OPR?

Response:

The FBI's Office of Professional Responsibility (OPR) suspended the SIA for 14 days.

d. What is this employee's current employment status and assignment?

Response:

The employee is currently a non-supervisory Intelligence Analyst assigned to the Las Vegas Division.

e. Did this employee have a security clearance? If so, what level and what is the status of that clearance presently?

Response:

The employee had and continues to have a Top Secret security clearance.

18. The OIG also conducted an investigation between October 2012 and March 2013 in which a FBI Assistant Special Agent in Charge (ASAC) was found to be engaged in a personal relationship with a subordinate. The investigation also revealed that the ASAC willfully ignored a former SAC's instruction to terminate the relationship; that the ASAC and subordinate misused an FBI vehicle and FBI-issued Blackberry devices in furtherance of the relationship; and that the ASAC had given the subordinate gifts and money in violation of FBI policy. The ASAC also failed to disclose the relationship during his FBI security re-investigation. The FBI agent was placed on a 60-day suspension and upon his request, was reassigned to a GS-13 position in the same field office.

These responses are current as of 8/26/13

a. How did the two FBI employees misuse the FBI vehicle in this relationship?

Response:

The Assistant Special Agent in Charge (ASAC) admitted that he misused the FBI vehicle to drive to the subordinate's home on several occasions. Although the investigative record compiled by DOJ's OIG does not indicate the exact mileage involved in the misuse, it suggests that the misuse was minor. The ASAC and the subordinate admitted to engaging in sexual activity in the vehicle on two occasions, once in 2006 and once in 2009.

b. Did the FBI provide records for the agents' government issued gas cards to the DOJ OIG?

Response:

The case involved only one agent, the ASAC. The subordinate was not an agent. If DOJ's OIG asked the FBI for the ASAC's credit card information, this information would have been provided. The investigative file referred by DOJ's OIG to the FBI's OPR for adjudication did not contain credit card information.

c. How did the FBI agents misuse their FBI-issued Blackberry devices?

Response:

The ASAC and non-agent subordinate misused their Blackberry devices by sending sexually explicit text messages to each other.

d. At what financial cost were the above misuses passed to the taxpayer?

Response:

The Blackberry misuse did not result in financial cost. The financial cost of the Bureau vehicle misuse is unknown but is believed to be relatively minor in view of the limited number of trips and distances involved.

e. How many FBI agents were found to have misused their FBI-issued Blackberry devices in the same timeframe (October 2012-March 2013)?

Response:

Four.

These responses are current as of 8/26/13

f. Was the female subordinate found to have received any bonuses or financial benefits from the FBI during the timeframe of their relationship?

Response:

No.

g. In what form was the FBI security re-investigation in which the ASAC failed to disclose his relationship done (verbal or written)? Was there ever discussion between the OIG and FBI about prosecuting the ASAC for an 18 USC 1001 charge?

Response:

FBI security reinvestigations contain both written and oral components. Both DOJ's OIG and the FBI's OPR reviewed the security reinvestigation statements made by the ASAC regarding his relationship with a subordinate. The reinvestigation question was whether the ASAC had engaged in activity that could make him vulnerable to pressure, raise questions about his trustworthiness, or cause embarrassment to the federal government. DOJ's OIG, which investigated the matter, found that the ASAC's negative responses constituted a failure to be frank in an official document. The FBI's OPR, which adjudicates misconduct based on the information developed through investigation, credited the ASAC's statement that he answered truthfully and did not recognize the need to disclose his relationship in this context because he did not feel he was vulnerable, untrustworthy, or a cause for embarrassment. OPR noted that the ASAC was not questioned about a specific incident or act of misconduct; rather, he was responding to a broadly worded questionnaire.

The FBI's OPR is not aware of any conversation between DOJ's OIG and the FBI regarding prosecution of the ASAC for a violation of 18 U.S.C. §1001. The OIG did not present its investigative results regarding the ASAC to a U.S. Attorney for prosecution.

19. Six months ago, I wrote you regarding the resignation of Director of Central Intelligence (DCI) David Petraeus and the involvement by the U.S. Department of Justice (Department), including the Federal Bureau of Investigation (FBI), in uncovering information that revealed an extramarital affair cited by General Petraeus as a reason for his resignation. My letter requested a briefing similar to the one provided to members of the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and Chairman Leahy of the Senate Committee on the Judiciary at that time.

On June 6, 2013, I received a letter from the Department of Justice stating, "Inasmuch as this is an ongoing investigation and significant individual privacy interests

These responses are current as of 8/26/13

are implicated, we are unable to provide you with a briefing or provide answers to...your letter." Aside from the issue that the Chairman of the Judiciary *was* provided a briefing despite the reasons listed above while I was not, it is my understanding that there were two investigative inquiries being conducted regarding the Petraeus matter. One inquiry was criminal while the other pertained to matters of National Security.

It is my understanding that the investigation regarding National Security is still ongoing. However, based upon the declination letter sent to Paula Broadwell in December and the statement of Department spokesman William C. Daniels, it appears that the criminal case is closed. According to Daniels, "After applying relevant case law to the particular facts of this case, the United States Attorney's Office for the Middle District of Florida has decided not to pursue a federal case regarding the alleged acts of 'cyber-stalking' involving Paula Broadwell." Inasmuch as it appears the criminal case is closed, I resubmit my requests regarding the *criminal* matter once again. Please provide:

- a. A timeline of events from initial contact with FBI personnel through the close of the criminal inquiry.
- b. An explanation of how and why the FBI opened the criminal inquiry.
- c. A detailed list of personnel who signed off on the criminal investigation.
- d. A detailed account of the legal authorities used to obtain each of the electronic communications of those involved including NSLs and Exigent Letters, and the role, if any, of any U.S. Attorneys' Offices.
- e. An explanation of the timing and circumstances of how you first learned of this criminal inquiry and when the White House was notified of the inquiry.
- f. A description of Department employees' contacts with Congress prior to the election and whether the Department considers those contacts protected whistleblower disclosures.
- g. An explanation of whether the FBI shared information regarding the criminal investigation with investigators or protective security details from various military criminal investigation organizations (including the CIA, Army Criminal Investigation Command (CID), Air Force Office of Special Investigations (OSI), or Navy Criminal Investigative Service (NCIS)) and when that information was shared.
- h. A description of the status of any related reviews being conducted by the FBI Inspections Division, the Office of Professional Responsibility, the Deputy Attorney General's Office, or the Office of Inspector General, including any related to public reports

These responses are current as of 8/26/13

of alleged communications between an FBI agent and any witnesses that involved inappropriate photographs or text.

- i. An explanation of whether the extramarital affair was uncovered during the initial background investigation conducted by the FBI prior to General Petraeus' confirmation as DCI.**
- j. An explanation of any legal analysis conducted by any component of the Department, including the FBI, regarding whether you or the FBI Director were obligated by law to report the investigation of DCI Petraeus to the President or any other government official.**

Response to subparts a through j:

While DOJ may have declined to prosecute Paula Broadwell for specified offenses, this does not mean the Department has reached this determination as to all activities or persons involved. In fact, the criminal investigation is ongoing and, as the question recognizes, DOJ policy generally precludes the FBI from commenting on the status of ongoing investigations and from disclosing nonpublic information about such investigations.

20. I understand that enforcing the Controlled Substances Act is not the primary mission of the Federal Bureau of Investigation. However, the FBI does have the authority to investigate drugs and drug trafficking and enforce the Controlled Substances Act.

As you may be aware the states of Colorado and Washington recently passed ballot measures that legalize the possession of small amounts of marijuana for recreational use. These ballot measures are in direct conflict with the Controlled Substances Act.

- a. Do you believe the Controlled Substances Act should be enforced?**

Response:

Yes. The FBI continues to investigate violations of laws within our jurisdiction, including violations of Title 21 of the U.S. Code, in accordance with DOJ policies. We also continue to collaborate with our partner agencies, including the Drug Enforcement Administration (DEA) and DHS's component agencies, to enforce the laws regarding which we have concurrent jurisdiction.

- b. Do you support the legalization of marijuana for recreational or any other use?**

Response:

These responses are current as of 8/26/13

The FBI would be pleased to provide its views of possible legislation on this topic to DOJ pursuant to DOJ's role in assisting in the development of the Administration's position.

c. What do you believe the impact of marijuana legalization is?

Response:

The FBI is not in a position to assess the impact of state laws that legalize and regulate marijuana production, possession, use, sale, or related activities.

21. Over the past three years, I have sent numerous letters of inquiry to HUD raising concerns about wasteful spending and possible criminal activity at the PHAs across the country. The FBI has investigated fraud and theft of funds by top housing authority executives, managers and even Board members who have used the funds to pad their own pockets, reward their friends and family, and pay off others to look the other way.

These investigations have been vital for identifying employees who are abusing the public trust and halting further abuse of federal dollars. While I do not want to interfere with ongoing criminal investigations, I believe that this information must be available to the general public, not just the media, to bring greater transparency to how taxpayer dollars are being spent. Therefore, I am requesting the following information:

- a. What agreement(s) is(are) in effect between HUD and the FBI that dictate when the FBI may begin a criminal investigation? Please provide a copy of the agreement(s).**
- b. What criteria are required for the FBI to conduct a criminal investigation at a public housing authority?**

Response to subparts a and b:

As the primary investigative agency of the federal government, the FBI has the authority to investigate all violations of federal law that are not exclusively assigned to another federal agency. In addition, though, pursuant to the Inspector General Act of 1978 (as amended), the Housing and Urban Development (HUD) OIG conducts and supervises civil and criminal investigations relating to HUD's programs and operations; promotes economy, efficiency, and effectiveness in the administration of HUD programs and operations; and prevents and detects fraud and abuse in HUD's programs and operations, among other things.

The FBI's investigative activities are governed by the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) and the FBI's DIOG. The FBI may initiate

These responses are current as of 8/26/13

investigative activities as authorized by those guidelines. For example, as a general matter the FBI may open a preliminary investigation to detect, obtain information about, or prevent or protect against federal crimes when an approving official determines there is adequate predication, and we may open a full investigation if there is an "articulable factual basis" concerning possible criminal activity.

c. Please provide a list of the housing authorities the FBI has investigated during the previous five years, as well as the disposition for each.

d. Please document the housing authorities the FBI declined to investigate and why.

Response to subparts c and d:

The FBI does not track the number of public housing agencies, or individuals serving in those agencies, that have been subjects of FBI investigations. As indicated above, we are authorized to engage in investigative activity only if there is adequate predication, as required by the AGG-Dom and the DIOG.

These responses are current as of 8/26/13

